Sébastien Dumoulin

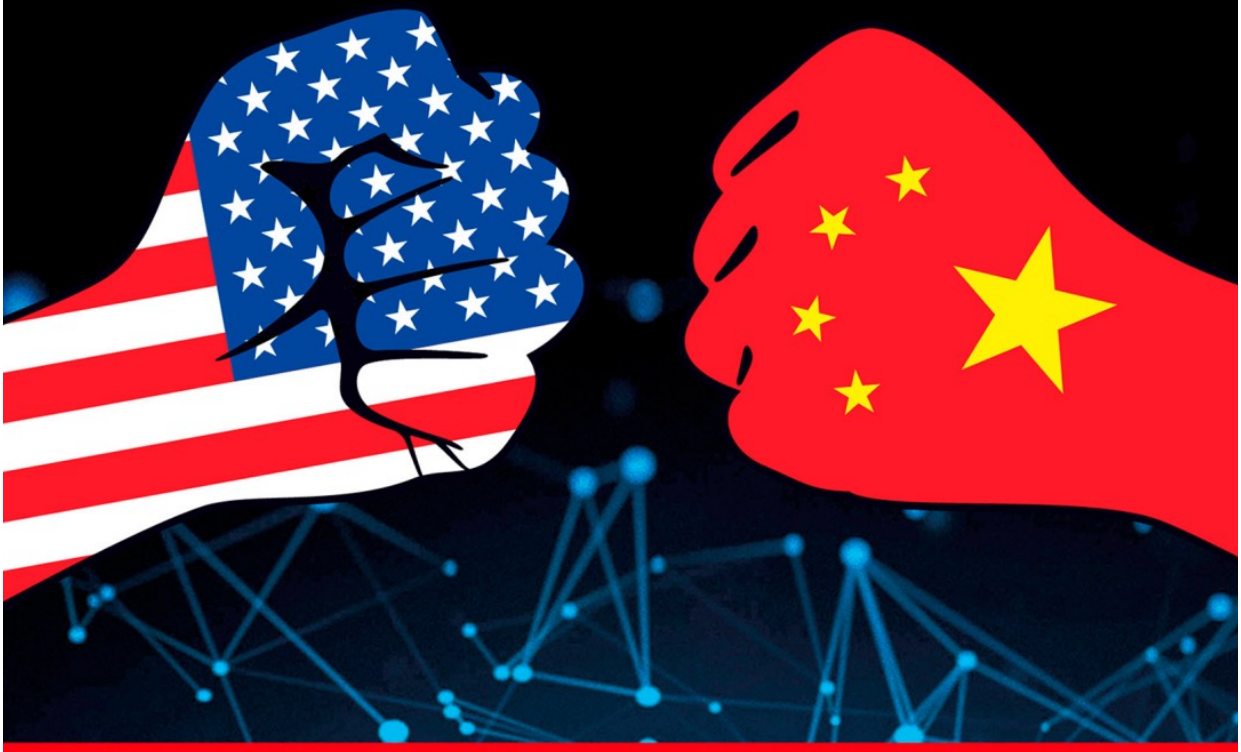
LA GUERRE MONDIALE DES ONDES

Le roman d'espionnage de la 5G

Tallandier

Sébastien Dumoulin

LA GUERRE MONDIALE DES ONDES



Le roman d'espionnage de la 5G

Sébastien Dumoulin

La Guerre mondiale des ondes

Le roman d'espionnage de la 5G

Tallandier

© Éditions Tallandier, 2021
48, rue du Faubourg-Montmartre – 75009 Paris
www.tallandier.com

EAN : 979-10-210-4681-8

Ce document numérique a été réalisé par Nord Compo.

À Marine, pour sa vigilance,
sa bienveillance et son abnégation.
Aux petites mains de Bouguenel,
pour leur soutien solide et discret.
Au trio Mizroulin, pour les rires et les cernes.

SOMMAIRE

Titre

Copyright

Dédicace

Avant-propos

Chapitre premier - De grandes espérances

Chapitre II - La fusée Huawei

Chapitre III - Un groupe pas comme les autres

Chapitre IV - Des réseaux et des espions

Chapitre V - Les vieilles rancœurs de l'Oncle Sam

Chapitre VI - Le Blitzkrieg de Washington

Chapitre VII - Les dominos

Chapitre VIII - La question idéologique

Chapitre IX - Le monde d'après

Conclusion

Notes

Avant-propos

La femme traverse des halls quasi déserts. Il est près de midi à l'aéroport international de Vancouver, ce samedi 1er décembre 2018, mais les zones de contrôle des douanes, dont la majorité des voyageurs ignorent jusqu'à l'existence, sont tranquilles. D'un pas leste permis par son survêtement bleu marine, elle suit une petite fonctionnaire dont l'imposante chevelure rousse ramenée en queue-de-cheval ne fait pas oublier le sérieux de l'uniforme. La femme rajuste son sweat-shirt. Ses cheveux noirs sont lâchés sur ses épaules. Sans doute est-elle lasse de sa demi-journée de vol depuis Hong Kong. D'autres images des caméras de vidéosurveillance de l'aéroport la montrent un peu plus loin[1], les mains dans les poches, face à deux agents aux frontières occupés à fouiller ses bagages, empilés sur un chariot à proximité. La scène a toutes les apparences d'un contrôle de routine. Ce n'en est pas un. La quadragénaire, arrêtée, menottée et placée dans un fourgon à destination d'un centre correctionnel canadien, n'est pas une vulgaire criminelle. Il s'agit de la directrice financière de Huawei, numéro 1 mondial des télécoms et fleuron technologique chinois. Et accessoirement de la propre fille de son fondateur. Pour Pékin, l'affront est impardonnable. Et nul ne s'y trompe : le Canada a fait le sale boulot, mais les États-Unis sont à la manœuvre. Pourquoi les Américains menacent-ils de placer la femme

d'affaires derrière les barreaux pour plusieurs dizaines d'années ? Est-ce une simple question de droit ? Ou, comme le pensent de très nombreux observateurs, une tentative brutale d'entraver l'ascension technologique de la Chine ?

Le moment n'est pas neutre. Le monde est sur le point de basculer dans la 5G – un nouveau réseau de télécommunications dont Huawei est le spécialiste et qui doit bientôt révolutionner nos sociétés en connectant des milliards d'objets intelligents en temps réel. Les opérateurs télécoms en rêvent : « Prêts pour une nouvelle révolution ? », demande une publicité pour Orange en France, « Ça va tout changer », clame Verizon aux États-Unis, « Le futur est là », renchérit Three au Royaume-Uni dans une vidéo regorgeant d'hologrammes et de jeux vidéo immersifs. Pour l'industrie des télécoms, la 5G est une opportunité en or. Les consultants de McKinsey font miroiter plus de 2 000 milliards de dollars de retombées économiques d'ici 2030[2]. Certes, aujourd'hui, la 5G n'est qu'un petit sigle qui s'affiche sur l'écran des smartphones les plus récents. Mais demain, entreprises, villes et États s'en serviront pour piloter des flottes de voitures autonomes, des escadrilles de drones ou des batteries de robots industriels. Pour ses promoteurs, la 5G est la porte d'entrée vers le « tout connecté », la clé de la « troisième révolution industrielle » – celle du numérique et des énergies vertes imaginée par l'économiste Jeremy Rifkin.

La promesse est belle. À moins qu'en guise de troisième révolution industrielle, la 5G ne provoque une troisième guerre mondiale, ou en tout cas un conflit majeur entre les États-Unis et la Chine, les deux puissances technologiques du XXIe siècle et les deux premières économies de la planète. Car si pour la Chine, la 5G est un levier pour prendre l'ascendant sur son rival, du côté américain, tous les moyens sont bons pour torpiller ce plan. Washington bat activement

le rappel de ses alliés, jouant la carte politique et sécuritaire là où Pékin pèse de tout son poids économique. Sommée de choisir, l'Europe est embarrassée. L'Inde s'aligne. L'Afrique fait l'autruche… Jamais depuis bientôt un demi-siècle une telle fracture ne s'était ouverte. Un nouveau rideau de fer, technologique, s'abat sur le globe. Pourquoi la 5G a-t-elle précipité sa descente ? Quel rôle joue Huawei, cette entreprise à la réussite insolente devenue en vingt ans le fer de lance de la tech chinoise et la bête noire des services secrets américains ? Pour le comprendre, il faut essayer d'éclairer un peu le monde des espions – de toutes nationalités – qui fourmillent dans l'ombre des réseaux télécoms. L'information y est parcellaire, les tentatives de manipulation omniprésentes, les incertitudes nombreuses. Ces difficultés, avec lesquelles l'ouvrage compose au mieux, ne peuvent cacher le caractère unique de ce conflit, où des milliards de dollars de contrats vont s'évaporer, des ministres se faire menacer, des citoyens se faire embastiller ou jeter dans le couloir de la mort… La guerre mondiale des ondes a commencé. Voici comment.

CHAPITRE PREMIER

De grandes espérances

Le ramdam autour de la cinquième génération de réseaux mobiles, ou 5G, est justifié par ses promesses étonnantes. Surpuissant, hyper-réactif, adaptable… c'est le réseau de tous les superlatifs. Du côté des acteurs des télécoms, c'est le moment de la partie de poker où il s'agit de faire tapis. Économiquement, tous veulent rafler la mise. Mais lorsque les enjeux financiers et sociétaux s'envolent, les risques pour la sécurité augmentent aussi…

Une décennie d'attente

Barcelone semble prise d'assaut. Les hôtels du centre-ville sont bondés. Des files de taxis encombrent les principales artères de la cité catalane. Ce 22 février 2016, le Mobile World Congress, la grand-messe annuelle des télécoms, ouvre ses portes. Et la jauge des organisateurs s'affole. Pour la première fois, la barre des 100 000 visiteurs a été franchie. À l'exception d'Apple, qui snobe ostensiblement le salon, toute l'industrie est là : constructeurs de téléphones, opérateurs, fabricants de puces électroniques ou

d'antennes mobiles… Tous ont les yeux rivés sur la 5G, la nouvelle technologie de réseaux mobiles qui doit ringardiser la 4G dès 2020. Il reste quatre ans pour se préparer. Chacun se rode et vient prendre le pouls des concurrents.

L'avènement d'une nouvelle génération mobile n'a rien d'anodin. Ce type de bascule technologique ne se produit que tous les dix ans. Dans les années 1980, les réseaux 1G permettaient à quelques privilégiés de passer des appels depuis leur automobile. La 2G des années 1990 a démocratisé le téléphone mobile, avec son cortège de SMS et de smileys stylisés. Les années 2000 ont apporté la 3G, qui permet d'échanger des données en plus de la voix. Enfin, depuis 2010, la 4G a dopé l'Internet mobile aux stéroïdes avec du haut débit permettant de regarder des films en streaming ou de passer des appels vidéo depuis un smartphone.

À Barcelone, chacun sait que le compte à rebours est lancé. Dans les allées du salon, le sigle « 5G » est partout. Impossible d'y échapper. De l'Allemand Deutsche Telekom au sud-coréen SK Telecom en passant par le géant britannique Vodafone, tous les opérateurs veulent montrer qu'ils sont dans les starting-blocks, prêts à dépenser – comme tous les dix ans – des centaines de milliards d'euros.

Un chèque de plusieurs milliards

Cet énorme chèque servira dans un premier temps à payer et installer de nouvelles antennes. Tous les pylônes – qu'il s'agisse des grands squelettes de métal dans les campagnes ou des toits d'immeubles loués pour y placer des émetteurs en centre-ville – seront progressivement équipés de nouveaux boîtiers 5G. Il faut aussi souvent renforcer les mâts eux-mêmes, pour supporter la surcharge,

et relier chacun d'entre eux avec une fibre optique dédiée (ou plutôt deux, par sécurité, au cas où l'une serait accidentellement endommagée) pour doper les débits. Techniquement et financièrement, le chantier est immense, même s'il est lissé sur une dizaine d'années.

Si l'on ne regarde que la France, les opérateurs investissent 3 milliards d'euros par an dans leurs réseaux mobiles, soit l'équivalent d'un porte-avions de nouvelle génération tous les deux ans. Et cela sans même parler du coût des fréquences radio utilisées pour diffuser le signal. À l'automne 2020, Orange, SFR, Bouygues Telecom et Free se sont affrontés pendant trois jours dans une enchère en ligne pilotée par l'Arcep (Autorité de régulation des communications électroniques, des postes et de la distribution de la presse) pour finir par verser à Bercy 2,8 milliards d'euros – l'équivalent d'une année entière d'investissements – en échange de nouvelles fréquences dédiées à la 5G. Et encore, les opérateurs français s'estiment chanceux. En Allemagne et en Italie, les enchères ont traîné en longueur, aucun opérateur ne voulait lâcher le morceau, et la facture a dépassé les 6 milliards d'euros.

Du côté des constructeurs d'antennes, on est également dans les starting-blocks. Trois grands groupes se partagent l'essentiel du marché mondial des équipements de réseaux mobiles – le finlandais Nokia, le suédois Ericsson et le chinois Huawei. Plus encore que le reste de l'industrie, le géant asiatique mise très gros sur la 5G. À l'entrée du Mobile World Congress de Barcelone, chaque visiteur s'est vu remettre un badge à son nom. Et, pour le porter en évidence, une sangle rouge à passer autour du cou. On y distingue sans mal le logo et le nom du sponsor : Huawei. La marque chinoise est ainsi omniprésente dans les allées. Sans compter qu'elle dispose d'un gigantesque espace d'exposition, où l'on peut manipuler ses

smartphones et autres tablettes mais aussi rencontrer, sur rendez-vous, cadres et experts du groupe.

L'un d'entre eux ne se fait pas prier. Avec sa boule à zéro et sa bonne humeur contagieuse, Mérouane Debbah est loin de l'image austère du chercheur en mathématiques. Le normalien dirige le laboratoire de mathématiques et d'algorithmes que Huawei a établi à Boulogne-Billancourt, en région parisienne. Son équipe de 70 chercheurs est parmi les plus avancées au monde dans un domaine très particulier : les équations qui régissent les réseaux de télécommunications.

Leur sujet numéro 1 est inévitablement la 5G. Excellent pédagogue, le scientifique est ravi d'en décrire les fondamentaux au néophyte et de lui offrir un aperçu du futur. « Grâce à la 5G, nous avons atteint 115 gigabits par seconde [Gbs] en laboratoire », sourit-il, guettant la réaction de son interlocuteur, à qui il faut une brève pause pour digérer l'information. Bien sûr, ces résultats en salle blanche n'ont aucune chance de se reproduire en conditions réelles dans l'immédiat, mais la simple promesse d'atteindre 1 Gbs – soit cent fois moins – suffit à faire briller les yeux des technophiles. C'est l'équivalent de ce qu'offre la fibre actuellement dans les foyers, mais sans fil. Avec un bon smartphone et une antenne à proximité, la 4G délivre dans le meilleur des cas quelques dizaines de mégabits par seconde – soit un rapport d'un à cent. Et encore, dans les allées d'un salon très fréquenté comme celui de Barcelone, les réseaux saturent face au trop grand nombre de connexions et il est tout bonnement impossible de se connecter à Internet avec son téléphone. Mais promis, la 5G va changer tout cela, et bien plus.

Un pied dans le futur

Moins de trois ans après la présentation du chercheur en mathématiques à Barcelone, son employeur Huawei en a fini avec les démonstrations de laboratoire. Ses premières antennes 5G sont mises à contribution pour des expérimentations grandeur nature. Fin 2018 à Fuzhou, dans le sud-est de la Chine, un homme vêtu d'un élégant costume bleu est assis sur une chaise de bureau face à deux grands écrans, tandis que, tout autour de lui, photographes et caméramans immortalisent la scène. Les deux mains posées sur des sortes de joysticks, le docteur Liu Rong contrôle des bras robotisés qui, à 50 km de là, procèdent à une lobectomie hépatique – l'ablation d'un morceau du foie – sur… un cochon. À en croire la presse chinoise[1], il s'agit d'une première mondiale. Non pas que la chirurgie à distance soit une nouveauté. Vingt ans plus tôt, des médecins ont déjà procédé, depuis un hôpital de Strasbourg, à l'ablation de la vésicule biliaire d'une patiente allongée à New York, grâce à des robots connectés en fibre optique. Mais c'est la première fois qu'une telle opération s'effectue par la voie des ondes hertziennes, grâce à la 5G. Encore quelques mois et c'est un patient humain, atteint de la maladie de Parkinson, qui se voit implanter un neurostimulateur par un robot sans fil, piloté en 5G. L'opération a lieu à Pékin, mais le chirurgien est à 3 000 km de là, dans le sud du pays[2]. Dans les deux cas, ces démonstrations spectaculaires n'ont pas d'intérêt médical particulier. En revanche, elles prouvent l'extraordinaire réactivité et robustesse de la 5G – qui pourra demain servir à des opérations chirurgicales dans des zones difficiles d'accès ou sur des terrains d'opérations militaires, mais aussi à quantité d'autres applications.

Car la 5G est potentiellement porteuse d'innovations et de changements sociétaux bien plus grands que les générations précédentes – au point que le patron de Nokia France semble regretter sa dénomination. « La 5G a un problème de nom, explique

Thierry Boisnon. Ce n'est pas une simple évolution de la 4G[3]. » Certes, les débits vont être démultipliés. Il sera possible de télécharger dans la rue le dernier épisode de sa série préférée en moins de temps qu'il n'en faut pour le dire. Mais ce n'est que la partie émergée de l'iceberg. La 5G dispose de trois autres atouts révolutionnaires. Le premier est sa capacité à accueillir des milliers de connexions sur un même site. De quoi permettre aux spectateurs d'un match de football, par exemple, de ne jamais connaître la frustration de n'avoir « aucune barre » sur l'écran de leur smartphone en raison de la saturation des réseaux. De quoi, surtout, connecter en plus des téléphones des millions de capteurs pour mesurer et optimiser des pans entiers de l'activité humaine : les réseaux d'énergie, la circulation dans les villes…

Deuxième évolution majeure, la 5G permettra aux opérateurs de découper, grâce à des logiciels, le réseau en « tranches » virtuelles pour garantir la priorité à certains utilisateurs. Impossible à l'heure actuelle pour les pompiers par exemple d'échanger des informations sur le réseau 4G – le risque est trop important qu'à l'occasion d'un événement comme l'incendie de Notre-Dame, la foule des curieux filmant la scène avec leur smartphone n'engorge le système. Dans les aéroports, pour la signalisation ferroviaire… partout où des communications industrielles sont incompatibles avec les aléas d'un réseau télécoms public, ce sont des réseaux privés souvent datés, reposant sur d'autres technologies radio bien moins avancées, qui sont utilisés faute de mieux. Grâce aux « tranches » virtuelles, il sera possible de les assurer en 5G en toute sécurité.

Enfin, troisième changement clé, le nouveau réseau bénéficiera d'une très faible latence, c'est-à-dire d'un temps très court entre l'envoi d'un signal et la réponse. Sur un réseau 4G, l'information met quelques dizaines de millisecondes à faire le voyage aller-retour

depuis un smartphone jusqu'au serveur qui contient les données demandées. L'utilisateur ne s'en rend quasiment pas compte. C'est à peine plus lent que notre cerveau, qui met, lui, quelques millisecondes à traiter une information. L'objectif de la 5G est de faire beaucoup mieux, en abaissant la latence du réseau mobile sous le seuil d'une milliseconde. Ce n'est pas qu'une prouesse technique, quasi invisible à l'œil nu. Une telle réactivité, associée à la garantie de ne jamais avoir d'encombrement du réseau grâce aux « tranches virtuelles », ouvre la porte à quantité d'applications aujourd'hui inenvisageables en mobilité : des jeux vidéo et des concerts en réalité virtuelle, des files de camions ou des flottes de drones évoluant simultanément sans le moindre accroc…

La question des usages futurs de la 5G est délicate. Il est impossible de prédire avec exactitude les innovations qui germeront une fois le réseau en place. Exactement comme personne n'aurait su prévoir que la 4G permettrait l'émergence d'applications devenues aussi banales que Spotify ou Uber. Mais l'enjeu est bien plus élevé que par le passé. « Être en retard sur la 4G, c'est dommage. Sur la 5G, c'est grave, systémique, expliquait dès 2018 Sébastien Soriano, le président de l'Arcep – le régulateur français des télécoms. Toutes les industries perdraient la possibilité de se moderniser. La voiture connectée serait en retard, les ports, les usines[4]… »

Huawei bien positionné

Dans la course mondiale vers ce réseau futuriste, le Chinois Huawei est idéalement placé. Bien connu pour ses smartphones haut de gamme, le groupe de Shenzhen a historiquement une autre spécialité. Il construit des équipements de réseaux et autres antennes

de téléphonie mobile pour les opérateurs du monde entier. À la veille de l'avènement de la 5G, Huawei est même le numéro 1 mondial du secteur, avec environ un tiers du marché, devant deux autres poids lourds – le suédois Ericsson et le finlandais Nokia – et quelques acteurs de moindre envergure – son compatriote Zhongxing Telecommunications Equipment (ZTE) ou le sud-coréen Samsung. Avec des antennes dans 170 pays, Huawei se vante régulièrement de connecter un tiers de l'humanité.

Grâce à sa double activité – dans les appareils grand public et les équipements pour opérateurs –, Huawei est devenu un groupe gigantesque. Avec 123 milliards de dollars de revenus en 2019 – l'équivalent du PIB du Maroc –, il fait partie des 50 plus grosses multinationales du monde. Dans les technologies, il n'y a guère qu'Apple et Samsung à peser encore deux fois plus lourd, et Google (163 milliards de dollars de chiffre d'affaires) à le devancer encore d'une tête. Huawei fait la même taille que Microsoft ou que Facebook et Intel cumulés.

Ce n'est pas le seul groupe chinois à être un tel mastodonte. Mais à l'exception du groupe d'assurances Ping An, les autres géants chinois sont des entreprises d'État du BTP, de la banque ou de l'énergie. Dans le domaine technologique, Huawei est la star chinoise qui éclipse toutes les autres. Aux Gafa (Google, Apple, Facebook, Amazon) américains, il est devenu courant d'opposer les BATX chinois, constitués de Baidu (le moteur de recherche, équivalent de Google), Alibaba (la plateforme de distribution en ligne à la façon d'Amazon), Tencent (le groupe de jeux vidéo mobile et éditeur de la messagerie WeChat) et Xiaomi (le fabricant de smartphones). Il faudrait pourtant additionner les revenus annuels des quatre groupes pour constituer un rival comparable à Huawei. Et aucun d'eux

n'affiche la réussite à l'international de Huawei, dont 40 % des recettes viennent de l'extérieur de la Chine.

La performance est d'autant plus remarquable que l'entreprise, encore quasi inconnue en Occident il y a quinze ans, a mis moins de trente ans pour parvenir au sommet. Sa trajectoire météoritique l'a vue dépasser ses concurrents les uns après les autres. Dès 2009, le franco-américain Alcatel-Lucent et le finlandais Nokia (qui fusionneront par la suite) sont dans son rétroviseur. Huawei débarque alors sur la deuxième marche du podium, derrière Ericsson. En trois petites années, il ravit sa couronne de premier équipementier télécoms au vieux monarque nordique. Personne n'a semblé en mesure de la lui contester depuis.

Au contraire, alors même que ses concurrents souffrent du caractère cyclique des commandes de matériel télécoms, Huawei survole la crise grâce à ses ventes de téléphones qui explosent. Depuis 2018, il a relégué Apple en troisième position des fabricants de smartphones et Huawei lorgne ouvertement sur la position de leader que le Sud-Coréen Samsung occupe depuis 2012.

Solide techniquement et financièrement, Huawei voit s'avancer la vague de la 5G avec la sérénité d'un champion du monde. Sur les 50 plus grands opérateurs télécoms du monde, 46 sont ses clients. Il ne lui manque que les quatre groupes qui se partagent le marché américain : AT&T, Verizon, Sprint et T-Mobile. Mais même si ceux-là continuaient de le bouder, la 5G est vouée à entériner la domination du groupe chinois sur les télécoms mondiales.

Pluie de contrats

Colonnades, bas-reliefs, lustres en cristal… Les salons de l'hôtel Paris Monte-Carlo n'ont rien d'une salle de conférences high-tech. Le 9 juillet 2019, on y trouve pourtant tous les responsables numériques du gouvernement de Sa Majesté Albert II, mais aussi le milliardaire français Xavier Niel, le fondateur de Free, ainsi que Guo Ping, l'un des trois vice-présidents tournants de Huawei. Un écran géant a été installé dans le palace monégasque. C'est ici, sur la place du célèbre Casino, que la principauté est venue annoncer en grande pompe la couverture complète du Rocher en 5G. La prouesse est réelle. À l'époque, les grands pays européens n'ont même pas libéré les fréquences radio idoines pour les opérateurs. Mais elle n'est pas complètement inattendue. Monaco Telecom, propriété à 48 % de l'État monégasque et à 52 % de Xavier Niel, se fait fort d'être à la pointe de la technologie. Exerçant un monopole sur le petit État de 2 km^2, l'opérateur peut se permettre de faire payer plus de 100 euros ses forfaits à une clientèle très aisée. En retour, il a les moyens d'investir dans les antennes les plus modernes… ainsi que dans les techniques de camouflage pour transformer les pylônes disgracieux en palmiers et les fondre dans le paysage de carte postale de la principauté. Très attaché à son statut de vitrine technologique, Monaco Telecom ne pouvait naturellement pas rater la 5G, et s'est tourné vers Huawei, son partenaire historique.

Remporter ce genre de victoires de prestige est important pour le groupe chinois. Il faut montrer au monde qu'il dispose de l'ascendant technologique pour conserver sa place de numéro 1 mondial du secteur. Avec Nokia et Ericsson, Huawei se livre à une bataille de communiqués. C'est à qui annoncera le plus de contrats 5G. Début 2020, Huawei assure qu'il mène la danse, avec 91 clients opérateurs, dont 47 en Europe. Ses détracteurs pointent qu'un nombre de contrats ne signifie pas grand-chose en l'absence d'indication sur leur

volume. Mais au printemps 2020, une annonce colossale finit d'installer Huawei en pole position.

L'opérateur qui dévoile alors les résultats de son appel d'offres n'est pas n'importe lequel. China Mobile est le plus gros opérateur du monde, l'aîné des trois géants qui se partagent le marché chinois. À lui seul, il revendique un milliard de clients, soit deux fois la population totale de l'Union européenne. Nulle surprise à ce que les choix d'approvisionnement de ce mastodonte de l'industrie soient scrutés de près. Et ceux-ci sont encore plus radicaux qu'anticipés par les analystes. Son premier méga-contrat 5G, de plus de 5 milliards de dollars, est attribué à 57 % à Huawei et à 29 % à son compatriote ZTE. Le suédois Ericsson doit se contenter de 12 % du fabuleux magot, en dépit de prix plus attractifs. Tandis que Nokia repart les mains vides. Le propre responsable de la cybersécurité de Huawei aux États-Unis, Andy Purdy, se dira « déçu[5] » de cette attribution lourdement déséquilibrée en faveur de son employeur, estimant que le contrat donne des arguments à ceux qui dénoncent l'attitude protectionniste de la Chine sur ses propres marchés télécoms.

Plus largement, Huawei profite de la dynamique sans égale de la Chine dans les déploiements 5G. Si les États-Unis, la Corée du Sud ou le Japon ont commencé à voir fleurir les antennes de nouvelle génération, aucun pays au monde n'affiche les ambitions de Pékin. Poussés par les autorités, les trois opérateurs chinois ont quadruplé leurs investissements annuels pour couvrir avant la fin 2020 les 300 principales villes du pays. Ils ont prévu de mettre en service dans l'année 600 000 antennes 5G. C'est du jamais-vu alors que, dans l'ensemble de l'Union européenne, on ne compte alors qu'environ 400 000 pylônes de téléphonie, toutes générations confondues.

Chaque semaine, ce sont ainsi des milliers d'antennes qui sont installées dans toute la Chine. Même si la crise du coronavirus a un

peu ralenti le rythme général au premier trimestre 2020, les opérateurs en ont fait un levier de promotion de la technologie : des hôpitaux ont été équipés pour transmettre les scanners en 5G, des écoles et supermarchés ont été dotés de caméras thermiques 5G pour prévenir les potentiels malades, des drones 5G font respecter le confinement…

Selon la GSMA, l'association qui regroupe les opérateurs et équipementiers mobiles du monde entier, l'avance chinoise est écrite – 70 % des connexions 5G en 2020 se feront en Chine – et elle s'inscrit dans la durée – avec 180 milliards de dollars d'investissements prévus dans les cinq prochaines années, la Chine aura en 2025 un taux d'adoption du nouveau standard de téléphonie supérieur à 50 %, parmi les meilleurs du monde[6].

La peur du bouton rouge

Tout le monde ne saute pourtant pas de joie. En Europe en particulier, des mouvements anti-5G se développent – et bien plus durs que ce à quoi l'industrie avait été habituée avec les générations précédentes. Les craintes sanitaires de l'effet des ondes sur la santé humaine ressurgissent, malgré l'absence d'éléments scientifiques probants et l'adoption de normes d'exposition bien plus drastiques que les recommandations des autorités de santé. Des inquiétudes d'ordre environnemental s'y ajoutent. La 5G et son cortège de gadgets connectés sont-ils bien compatibles avec la réduction des émissions de CO_2 à laquelle se sont engagés les signataires de l'Accord de Paris ? De manifestations en recours juridiques, en passant par des demandes de moratoires locaux, la grogne monte.

Pourtant c'est une autre crainte qui taraude les autorités. Plus que les réticences d'une partie de la population civile, qui se traduisent ici et là par des incendies criminels de pylônes, ce sont les actions malveillantes d'acteurs étatiques ou de hackers chevronnés qui font trembler les services de sécurité. Car le corollaire d'une technologie qui doit être utilisée non plus seulement par des smartphones comme la 3G et la 4G, mais aussi par des millions de capteurs dans toute la chaîne de production, est qu'une panne ou un acte de sabotage aurait des conséquences dévastatrices.

Pirater un réseau 5G permettra, non plus seulement d'espionner des conversations, mais de perturber toute l'économie d'un pays, en mettant à l'arrêt ses réseaux de transport par exemple, ou en faussant certaines données critiques comme les remontées de capteurs de qualité de l'eau potable. Et, pourquoi pas, en cas de conflit ouvert, de simplement couper le réseau, plongeant dans le noir l'ensemble du tissu productif. Cette possibilité qu'un acteur externe dispose d'un « gros bouton rouge » pour éteindre la 5G a beau être très improbable techniquement, elle ne peut être complètement écartée. « Dans trois ou quatre ans, couper la 5G, cela reviendra à couper le courant en termes d'impact », explique Guillaume Poupard, le directeur général de l'Agence nationale de la sécurité des systèmes d'information (Anssi) dans une interview aux *Échos* début 2020. « Il ne faut pas être naïf et se dire que personne ne cherchera un jour à faire pression sur nous dans ces domaines-là[7]. »

Les maîtres espions ne sont pas paranoïaques sans raison. Ils savent qu'en 2015, une opération de piratage de grande ampleur, généralement attribuée à la Russie, a permis à de petits génies du code informatique de pénétrer les réseaux électriques ukrainiens et de plonger des centaines de milliers de foyers de l'ouest du pays dans l'obscurité, en plein conflit entre Kiev et Moscou à la suite de

l'occupation de la Crimée. Cette première mondiale – une cyberattaque se traduisant par des coupures d'électricité – n'a pas eu de répliques. Mais elle a montré la réalité de la menace. Depuis, les alarmes n'arrêtent pas de sonner. Les experts qui se sont penchés sur les réseaux électriques ukrainiens assurent que des programmes identiques visaient des compagnies ferroviaires et minières du pays. Ailleurs dans le monde, la présence de pirates est régulièrement détectée dans certaines infrastructures critiques comme les réseaux d'électricité ou bancaires. En 2016, les États-Unis inculpaient nommément sept pirates iraniens[8]. L'un d'eux s'était infiltré dans l'ordinateur de contrôle d'un petit barrage hydraulique de l'État de New York. « Cet accès aurait permis à l'inculpé de contrôler les niveaux d'eau et le flux hydraulique, faisant courir un danger clair et immédiat à la population », expliquait alors la ministre de la Justice, Loretta Lynch. En France, le patron de l'Anssi le répète conférence après conférence : il y aura un jour des morts à la suite de cyberattaques. La question est de savoir où et combien.

La 5G renforce ce risque, car ce que les spécialistes appellent la « surface d'attaque » augmente énormément : chaque objet connecté au réseau est un potentiel vecteur d'intrusion à contrôler. Les éléments centraux du réseau eux-mêmes sont moins faciles à surveiller. « La 5G utilise beaucoup, beaucoup plus d'antennes, chacune avec un rayon de couverture beaucoup plus restreint », détaille Ian Levy, le directeur technique du NCSC – l'équivalent britannique de l'Anssi –, qui pointe l'impossibilité de garantir que toutes sont physiquement sécurisées. « Ces petites cellules se retrouvent dans des endroits bizarres comme au sommet des lampadaires, dans les immeubles et même dans certaines box d'opérateurs[9]. » *Idem* pour les serveurs centraux. Pour assurer la fameuse latence réduite de la 5G, promesse d'hyperréactivité qui

ouvre la voie aux véhicules autonomes notamment, il faut que le signal voyage sur la distance la plus courte possible. Même à la vitesse de la lumière au sein d'une fibre optique, l'information ne peut parcourir « que » 300 km en une milliseconde. Ou 150 km aller-retour. En France par exemple, il devient impossible de ramener tout le trafic dans les data centers des opérateurs en région parisienne pour le traiter. Un robot dans une usine du fin fond de la campagne française serait alors incapable de réagir en temps réel comme promis. Les opérateurs le savent. Il leur faut construire des dizaines de petits data centers de proximité, répartis à travers l'Hexagone, pour rendre possible ce miracle de l'instantanéité de la 5G. Mais, une fois encore, cela facilite le travail de possibles pirates.

La protection des réseaux télécoms n'est pas un sujet nouveau. En France, les opérateurs télécoms sont depuis quinze ans sur la liste secrète des quelque 200 OIV (opérateurs d'importance vitale) identifiés par l'État et tenus d'appliquer des mesures de sécurité particulières. Les services de sécurité sont néanmoins souvent sceptiques quant à la bonne volonté des opérateurs à se préparer au pire. « En réalité, les opérateurs sont peu incités à faire plus de sécurité qu'il n'est strictement nécessaire[10] », souligne Ian Levy, qui reconnaît que personne, même pas lui-même, ne se pose la question de la sécurité de son opérateur avant de souscrire un abonnement.

La 5G est comme un nouveau couteau de cuisine. Parfaitement affûté, il va permettre de couper les légumes beaucoup plus finement et rapidement que les vieilles lames d'il y a dix ans. Aucun chef ne s'en passerait au motif que le nouvel outil est « trop coupant » et dangereux ! Seulement, un commis mal luné pourrait s'en servir pour le loger entre ses omoplates… Alors mieux vaut s'assurer des casiers judiciaires de toute l'équipe en amont. C'est ce que les autorités réalisent avec la 5G : on ne peut pas la confier à n'importe qui. Cette

prise de conscience va les pousser à s'intéresser de plus près à l'extraordinaire ascension du numéro 1 mondial des télécoms. Ce qu'elles vont découvrir, en plongeant dans l'histoire de Huawei, les fait hésiter – aujourd'hui encore – entre l'admiration, la perplexité et la méfiance.

CHAPITRE II

La fusée Huawei

Comment expliquer la puissance actuelle de Huawei ? Parti de rien il y a une trentaine d'années, dans une Chine rurale et sous-développée, le groupe a fait preuve d'une détermination exceptionnelle pour concevoir ses propres produits, les exporter massivement et continuer d'innover pour ne pas être cantonné au rôle du fournisseur asiatique bon marché. Et la fortune a souri à l'audacieux : ses grands concurrents ont au même moment accumulé les ennuis. À moins que ce ne soit Huawei qui les ait provoqués ?

Dans les pas de Deng

Ce 1er septembre 1982 à Pékin, 1 600 délégués, venus des quatre coins de la Chine, se réunissent pour l'ouverture du 12e Congrès du Parti communiste chinois (PCC). L'événement quinquennal est le point d'orgue de la vie politique nationale. C'est ici que sont désignés les membres du Comité central et – *in fine* – l'équipe dirigeante du pays. La mort de Mao, six ans plus tôt, a refermé la tragique parenthèse de la révolution culturelle. Le nouvel homme fort du

régime n'est pas un idéologue, au contraire. « Peu importe qu'un chat soit noir ou blanc, du moment qu'il attrape les souris », balaie Deng Xiaoping. Alors que le dirigeant prononce le discours d'ouverture du Congrès, un obscur inconnu est tout ouïe dans l'assistance. Ren Zhengfei, un ingénieur de quarante-deux ans, a reçu la prestigieuse invitation au Congrès en remerciement d'accomplissements scientifiques. Mais c'est en tant qu'homme d'affaires qu'il va devenir l'une des personnalités les plus influentes du pays.

La doctrine de Deng Xiaoping est pragmatique. Le « socialisme aux caractéristiques chinoises » qu'il propose aux délégués du 12e Congrès comprend une ouverture progressive du pays au capitalisme. Des « zones économiques spéciales » sont définies, où la Chine lâche petit à petit la bride aux entreprises privées. L'une de ces zones est un petit port de pêche, Shenzhen, situé à quelques kilomètres au nord de Hong Kong, la richissime colonie britannique. Elle va devenir une mégalopole de 12 millions d'habitants et le poumon de la tech mondiale. L'une de ces entreprises est Huawei, le futur premier groupe de télécoms du monde.

Ren Zhengfei fonde Huawei en 1987. Avec cinq associés, l'ingénieur a réuni 21 000 yuans – l'équivalent de 5 000 dollars – pour lancer une activité d'importation de matériel de télécommunications. Son nom, « Huawei », peut se traduire comme « la réussite de la Chine ». Un tel patriotisme n'a rien d'inhabituel pour les premières entreprises chinoises qui se créent à l'époque. Alors que le pays est largement sous-équipé en réseaux téléphoniques et que des plans de modernisation sont lancés par les différentes villes et provinces, Ren Zhengfei pense qu'il est possible de se faire une place au soleil en revendant des commutateurs téléphoniques étrangers, achetés dans la ville voisine de Hong Kong. L'idée est

bonne, la PME grossit. Et, dans l'ombre, Ren Zhengfei et ses équipes préparent un grand coup.

Nuit et jour, les jeunes ingénieurs chinois mettent au point leur propre commutateur numérique. L'appareil, appelé C&C08, est mis sur le marché en 1993. La décennie qui s'ouvre est celle du boom de la téléphonie fixe en Chine et Huawei est prêt à se jeter dans la bataille. Seul hic : les grands donneurs d'ordre n'ont d'yeux que pour les équipementiers occidentaux – Ericsson et Nokia, mais aussi Alcatel, Nortel, Lucent et Siemens. Personne ne veut prendre le risque d'acheter un produit local, fabriqué par un importateur de Shenzhen, même pour un tiers du prix affiché par la concurrence. Le *made in China* n'a alors pas bonne presse, surtout pour du matériel high-tech.

Pour surmonter cette difficulté, Ren Zhengfei formule une théorie, qui semble tout droit sortie d'un manuel maoïste : l'encerclement des villes par les campagnes. Autrement dit, plutôt que de s'acharner à démarcher en vain les grands clients des métropoles, Huawei va s'adresser aux zones rurales, un segment du marché délaissé par ses grands concurrents internationaux. Transportés parfois dans des conditions rocambolesques à travers la Chine, les appareils de Huawei peuvent ainsi faire leurs preuves. Non seulement ils s'avèrent d'excellente qualité pour une fraction du prix des équipements étrangers, mais en plus, ils sont taillés pour l'environnement chaotique des campagnes chinoises d'alors. Huawei a par exemple conçu un module d'alimentation électrique pour faire face aux sautes de courant, ou encore, tout simplement, équipé ses armoires informatiques de grilles en haut comme en bas pour éviter l'intrusion de rongeurs. La manœuvre est un succès considérable. En quelques années, Huawei s'installe dans le paysage national. Il va pouvoir se lancer à la conquête du monde.

Un champion de l'export

Comme d'autres entreprises chinoises à succès, Huawei aurait pu continuer à se développer uniquement sur son gigantesque marché intérieur. À la fin des années 1990, l'économie chinoise a en effet largement décollé et les deux décennies qui suivent vont donner naissance à la deuxième puissance économique mondiale. Mais l'ambition de Ren Zhengfei est bien plus grande. De ses voyages, notamment aux États-Unis, le patron revient invariablement avec un sentiment de retard à combler sur les firmes technologiques étrangères et la conviction que, pour se hisser à un niveau d'excellence comparable, il faut sortir de Chine et affronter la concurrence internationale sur des marchés plus difficiles.

En 1997, dix ans après sa création à Shenzhen, Huawei ouvre son premier bureau étranger, en Russie. Cette année-là, Ren Zhengfei effectue aussi un long voyage aux États-Unis pour rencontrer des cadres de l'industrie et s'inspirer des géants technologiques américains. Le patron parcourt l'Amérique en bus, une valise de cash en main[1] : la Chine n'a pas encore de système de carte de crédit. L'année suivante, c'est au tour du Kenya, puis des pays du Sud-Est asiatique – en pleine crise économique – et du Moyen-Orient. La firme reproduit à l'échelle du globe la stratégie d'encerclement qui lui a si bien réussi. Elle attaque les marchés émergents, en espérant remonter vers les grandes économies – qu'elle vise explicitement. Dès 2001, Huawei pose ses valises au Royaume-Uni et aux États-Unis pour commencer les démarchages commerciaux sur les continents européen et américain. Dans son livre, *Huawei, une success-story à la chinoise*[2], Yang Shaolong, un ancien cadre du groupe, revient longuement sur les moyens considérables que Huawei consacre alors à son expansion internationale. Le groupe se paie des stands de

démonstration sur les grands salons internationaux. Pour montrer sa crédibilité, il envoie ses produits par conteneurs partout dans le monde (un programme baptisé « Nouvel Orient-Express ») pour appâter les clients, les convaincre d'effectuer une visite en Chine (un autre programme, baptisé « Nouvelles routes de la soie ») et leur montrer la transformation du pays, les infrastructures numériques de ses grands opérateurs et ses propres installations industrielles.

Dans les pays émergents, comme hier dans les campagnes chinoises, les produits de Huawei s'imposent rapidement. Grâce à un développement en Chine, à des coûts salariaux sans commune mesure avec ceux de ses grands concurrents, il est capable d'être très agressif sur les prix et affiche fréquemment une décote de 30 % sur les produits concurrents. Dans un article du *Financial Times* de 2005, intitulé « Huawei, le challenger de Chine », Bert Nordberg, un des cadres dirigeants d'Ericsson, explique que son entreprise ne descend jamais en dessous d'un seuil tarifaire rédhibitoire. Or, trois ans plus tôt, lorsqu'il a été pour la première fois confronté à Huawei, dans des pays comme le Laos et le Cambodge, les prix affichés par le fabricant chinois étaient… encore inférieurs à ce seuil. Grâce à cet argument massue, le matériel de Huawei devient peu à peu la norme dans certaines zones du globe, notamment en Afrique. Aujourd'hui présent dans 40 des 54 pays du continent, le groupe y a bâti une bonne moitié des réseaux de télécommunications. Au point que, pour de nombreux cadres de l'industrie, le miracle africain du mobile n'aurait sans doute jamais pu se produire sans le groupe chinois. Et le pire pour ses concurrents est que le matériel de Huawei est performant et robuste. Avec les années, le groupe a quelques réalisations spectaculaires à son actif, comme le réseau mobile de La Mecque en Arabie saoudite, la ville du plus important pèlerinage au monde, le Hajj. « Tous les autres opérateurs ont échoué avant nous lors de ce

rassemblement important, mais depuis que nous avons pris les choses en main, le soutien technique a toujours tenu bon, raconte avec fierté Ren Zhengfei. Entre 4 et 5 millions de musulmans éteignent leur portable avant la prière et puis, après celle-ci, tout le monde l'allume en même temps. Ces quelques millions d'authentifications qui ont lieu simultanément n'ont pas fait tomber notre réseau et tout s'est bien passé[3]. »

BT, une clé pour l'Europe

En Europe, la porte a été plus lente à s'ouvrir. Dès 2001, l'entreprise décroche pourtant un contrat avec le français Neuf Telecom pour participer à la construction du réseau fixe de l'opérateur. Pour s'imposer, le groupe chinois a joué gros : il a construit en partie le réseau et laissé les techniciens de Neuf le tester gratuitement pendant trois mois. L'affaire était dans le sac. Il faut toutefois attendre le 8 décembre 2004 pour qu'un premier choc ébranle réellement la forteresse Europe. Ce jour-là, toute la presse économique mondiale se passionne pour l'internationalisation d'un groupe chinois. Il s'agit de Lenovo, qui rachète alors pour 1,8 milliard de dollars les fameux PC Thinkpad du géant américain IBM. L'annonce éclipse un autre contrat, celui signé par Huawei pour un montant plus modeste de 400 millions d'euros avec le néerlandais Telfort. Mais pour l'avenir de la tech mondiale, c'est pourtant celui-là qui compte. Huawei vient de vendre son premier réseau mobile 3G au cœur de l'Europe, à la barbe d'Alcatel, Nokia et Ericsson.

Le *Financial Times* – la Bible des affaires sur le Vieux Continent – écrit alors : « L'essor de Huawei pose des questions aux implications mondiales. La Chine peut-elle remonter la chaîne de valeur, en

répliquant son énorme succès dans la fabrication d'entrée de gamme dans les industries de haute technologie ? Si c'est le cas, quelle est l'ampleur de la menace pour les leaders installés du secteur comme Alcatel, Cisco, Ericsson, Lucent et Nortel[4] ? » Aujourd'hui, la réponse est connue. Trois des cinq groupes cités n'existent plus en tant que tels. Les deux autres ont été largement distancés par Huawei.

Quelques mois après sa victoire au Danemark, Huawei fait officiellement son entrée dans la cour des grands en se voyant attribuer une part d'un colossal marché de refonte du réseau fixe de British Telecom (BT), baptisé « 21st Century Network » et évalué à 10 milliards de livres sterling. L'opérateur historique britannique ne tarit pas d'éloges sur la qualité technique de son nouveau « fournisseur stratégique ». Cette même année 2005, les revenus de Huawei à l'international dépassent pour la première fois ses revenus en Chine. Et Ren Zhengfei fait son apparition dans la liste des 100 personnalités les plus influentes du magazine *Time*.

BT n'est pas n'importe quel client. C'est l'un des premiers opérateurs mondiaux. Être sur la liste de ses fournisseurs est un gage de qualité qui va ouvrir à Huawei les portes des opérateurs de toutes tailles à travers le monde. Les plus grands noms du secteur succombent les uns après les autres : Vodafone, Orange… L'Europe devient un Eldorado pour Huawei et n'a pas cessé de l'être depuis. En 2019, il s'agit encore de son deuxième marché derrière la Chine, avec 30 % des ventes sur le Vieux Continent. La pilule est dure à avaler pour ses concurrents locaux. Mais symboliquement, Huawei les a enterrés dès 2009. Cette année-là, le groupe chinois a lancé le premier réseau 4G au monde… avec l'opérateur norvégien Telenor, c'est-à-dire en plein cœur de la Scandinavie, chez ses rivaux Nokia et Ericsson.

R&D

La grille du 103 rue de Grenelle, à deux pas de l'hôtel Matignon, dans le « Paris des ministères », cache une ravissante cour pavée en U. Ce 9 octobre 2020, le patron de la recherche de Huawei en France, Mérouane Debbah, y accueille, tout sourire, les quelques dizaines d'invités masqués – Covid oblige – qui ont bravé les averses automnales pour assister au coupé de ruban. Huawei inaugure le centre Lagrange de recherche en mathématiques et calculs, son sixième centre de R&D en France. Le lieu est symbolique. L'hôtel particulier du XVIIIe siècle a été construit pour le ministère de l'Intérieur et les services télégraphiques nationaux. Le bâtiment du fond est encore coiffé du télégraphe de Chappe, un système de bras articulés considéré comme le tout premier système de télécommunications. Par la suite, le « 103 Grenelle » accueillera le premier ministère des Postes et Communications, mais aussi l'Office de radiodiffusion-télévision française (ORTF) qui y tournera la première émission télévisée de l'Hexagone en 1935, ou encore des bureaux de France Telecom jusqu'au début des années 2000. S'inscrire dans cette filiation ne peut que ravir Huawei. Quelques rieurs s'amusent que, sur le trottoir d'en face, la façade rouge d'un restaurant chinois affiche « Le Grenelle de Pékin ».

L'ambition du centre Lagrange, qui doit accueillir une trentaine de chercheurs permanents sur les 730 m^2 du deuxième étage du bâtiment, est de « repousser les limites fondamentales » des mathématiques, affirme sans ciller Mérouane Debbah – citant la limite de Shannon ou la loi de Moore. Les équipes bénéficieront d'une liberté académique totale. Et les premiers résultats ne seront pas attendus avant… dix ans. Huawei voit loin et sait son intérêt. Dans une vidéo projetée pour l'occasion, William Xu, le patron mondial de

la recherche de Huawei, explique qu'« au cours de ces trente dernières années, les mathématiques ont joué un rôle clé dans le développement des communications ». Mérouane Debbah renchérit : l'ambition du centre Lagrange n'est pas seulement de voir éclore des médaillés Fields – l'équivalent du Nobel en mathématiques, dont l'un des lauréats français, Pierre-Louis Lions, a accepté de présider le conseil scientifique du nouveau centre –, il s'agit de « jeter les bases de notre industrie pour les 50 prochaines années ».

En France, Huawei fait travailler plus de 200 chercheurs – un cinquième des effectifs de la filiale tricolore – sur des thématiques aussi diverses que les algorithmes, le design des téléphones ou le traitement d'images. Et ce n'est qu'un échantillon de la force de frappe mondiale du groupe de Shenzhen. Près de la moitié de ses quelque 200 000 salariés dans le monde travaillent sur la R&D. Huawei y a consacré en 2019 plus de 15 % de ses revenus, soit 18 milliards de dollars, ce qui en fait le cinquième investisseur mondial en R&D. À lui seul, Huawei dépense déjà davantage dans la recherche que ses principaux concurrents réunis. Et ce budget doit progresser pour atteindre 20 milliards de dollars en 2020. « Parce que nos salaires sont plus élevés que ceux des entreprises occidentales, nous avons attiré énormément de scientifiques étrangers qui viennent travailler pour Huawei, se félicitait Ren Zhengfei début janvier 2019. Nous avons au moins 700 mathématiciens, 800 physiciens, 120 chimistes, entre 6 000 et 7 000 experts spécialisés en recherches de base et plus que 60 000 ingénieurs supérieurs et ingénieurs de tous les domaines[5]. » Un profond respect pour les sciences est professé à la moindre occasion par le patron, qui est allé jusqu'à expliquer que sa propre fille, bien que membre du conseil d'administration, ne lui succéderait jamais à la tête de Huawei, faute d'une formation technique.

Le groupe sait soigner ses scientifiques. Le campus de Dongguan, non loin de son siège historique de Shenzhen, est emblématique. Ici phosphore une armée de 25 000 chercheurs, principalement des docteurs et des postdocs issus des meilleures universités. Ouvert début 2019, après trois ans de travaux et 10 milliards de yuans (1,3 milliard d'euros) d'investissement, le site s'étale sur 1,4 km^2 et abrite 108 bâtiments, répartis sur douze zones. Chacune est inspirée d'une ville européenne et un petit tram rouge – copie des trains qui parcourent les montagnes suisses – emmène en une dizaine de minutes des châteaux de Bavière aux vieilles maisons vénitiennes en passant par une réplique de la cité universitaire de Paris.

Ce focus sur la recherche remonte aux origines de l'entreprise et à ses efforts pour concevoir ses propres commutateurs. Au fur et à mesure que les revenus progressaient, Huawei a toujours augmenté en conséquence le budget de la recherche – autour de 10 % du chiffre d'affaires et même 15 % ces dernières années. En 2005, un des premiers rapports fouillés sur l'entreprise, réalisée par le think tank américain Rand Corporation[6] à la demande de l'US Air Force, fait une analyse qui ne se démentira pas : « Le secret de Huawei dans les premières années était très semblable à la formule utilisée par les Japonais dans les années 1960 et les Coréens dans les années 1970 : obtenir des technologies étrangères dans un premier temps, puis engloutir des sommes d'argent considérables en authentique R&D pour rester à la hauteur de la concurrence. » Pour les auteurs du rapport, il est indéniable que Huawei s'est plus qu'inspiré de ses grands concurrents à ses débuts. Mais ses propres investissements ont rapidement pris le relais. « Il attire aussi les meilleurs diplômés des universités de haute technologie chinoises, même si les salaires de départ sont 20 % inférieurs à ceux de Cisco, poursuivent les consultants. Les diplômés sont poussés à la place par l'appel

nationaliste d'une entreprise locale et la perte de salaire est quelque part compensée par les arrangements internes de répartition du capital d'une entreprise détenue par ses salariés. »

Très vite, Huawei comprend aussi l'intérêt d'internationaliser cet effort. En 1999, le groupe investit 400 millions de dollars dans un centre de recherche à Bangalore, La Mecque indienne du logiciel. Deux ans plus tard, des centres de R&D ouvrent dans la Silicon Valley et à Dallas, puis à Stockholm – à côté des labos d'Ericsson –, Londres, Moscou, Paris… Et les résultats suivent. En 2009, l'Organisation mondiale de la propriété intellectuelle classe Huawei en première position pour les dépôts de brevets internationaux. Dix ans plus tard, le groupe est toujours numéro 1, permettant à la Chine, pour la première fois, de passer devant les États-Unis. Ren Zhengfei a coutume de résumer ce succès par une expression militaire, bien connue en interne, la « charge de munition de Van Fleet » : « Dans la mesure où nous bombardons cette brèche de manière continue, progressivement, nous commençons à devancer les entreprises occidentales dans ce domaine bien précis[7]. »

Le travail de ses laboratoires se retrouve dans ses produits, avec des équipements particulièrement adaptés aux réalités de ses différents clients : antennes légères pour ne pas défigurer les bâtiments historiques des centres-villes de la vieille Europe, résistant aux températures extrêmes de la Scandinavie ou du Sahara, à l'humidité de la forêt amazonienne…

Parmi les innovations sorties des labos de Huawei qui parlent au grand public, il y a par exemple les petites clés 3G qui permettent de connecter un PC au réseau mobile. Parmi celles qui parlent aux opérateurs, il y a les logiciels grâce auxquels il est possible d'embarquer dans une même antenne différentes générations technologiques. Ces antennes dites « single RAN » seront une des clés

du succès phénoménal de Huawei en Europe. « Pour simplifier, Huawei proposait des équipements moins chers, plus légers, plus polyvalents et moins consommateurs d'énergie. Ils se sont vendus comme des petits pains », raconte un opérateur français.

Au début des années 2010, Huawei est pourtant encore vu comme le spécialiste du rapport qualité-prix, plus que de l'innovation. Un analyste de la banque Nomura voit même se dessiner un duopole sur le marché des équipements télécoms, avec Ericsson en tête de pont technologique et Huawei en pointe sur les coûts, pour permettre aux opérateurs de tempérer les prétentions tarifaires du Suédois[8]. Huawei a clairement fait mentir ce pronostic.

Fin 2019, avec 85 000 brevets à son actif, dont la moitié déposés en Europe ou aux États-Unis, Huawei estime avoir un des premiers portefeuilles mondiaux. Dès la définition du standard de téléphonie 3G, ses chercheurs ont œuvré à faire reconnaître leur travail par les autorités de normalisation. Avec la 4G, cette collaboration s'est renforcée. L'arrivée de la 5G marque un point culminant de cette stratégie. Huawei est non seulement le plus grand détenteur de brevets liés à la 5G, il s'est aussi imposé dans une catégorie clé, celle des brevets reconnus comme « essentiels » par les organismes internationaux. Parce qu'on ne saurait faire de 5G sans y avoir recours, ceux-ci sont mis à la disposition de tous les acteurs du marché à un tarif « juste, raisonnable et non discriminatoire », selon les règles de l'industrie. Mais cela se traduit *in fine* par des centaines de millions de dollars de royalties. Au lieu de vider les coffres de Huawei pour alimenter ceux des européens Nokia et Ericsson, ou ceux de l'Américain Qualcomm par exemple, comme c'était le cas pour les générations précédentes, la 5G va les remplir.

Ren Zhengfei, qui fait habituellement preuve d'une extrême modestie, ne peut s'empêcher de s'en montrer fier. « Beaucoup de nos

technologies dépassent de loin déjà celles des entreprises occidentales, non seulement dans les domaines de la 5G, d'optical switching et de puces optiques, se vante le patron début 2019. Nous disposons d'une quantité pharaonique de technologies d'une complexité incroyable, très avancées par rapport à celles des entreprises occidentales[9]. » Et pas question de se reposer sur ces lauriers. Dans les laboratoires de Huawei, on travaille depuis quelques années déjà sur la 6G en préparation de son arrivée autour de 2030.

Le prince des téléphones

La réussite de Huawei en trois décennies dans les équipements télécoms est phénoménale. Pourtant, l'entreprise a fait encore plus fort sur son deuxième marché, celui des terminaux. Pour se hisser en deuxième position des vendeurs de smartphones, il lui aura fallu… moins de quinze ans. Ce deuxième pilier de ses activités lui fournit une visibilité sans commune mesure auprès du grand public, désormais familier du célèbre logo aux huit pétales rouges qui orne chacun des 240 millions de téléphones qu'il a écoulés en 2019. Et ce business rapporte une petite fortune. Dès 2015, un quart des revenus proviennent des ventes de smartphones et autres PC siglés Huawei. En 2017, plus du tiers. En 2019, plus de la moitié, soit 67 milliards de dollars.

La partie était pourtant loin d'être gagnée. L'industrie du téléphone portable est extrêmement concurrentielle et ces vingt dernières années ont vu les marques les mieux installées s'évanouir. De façon remarquable, les grands industriels des équipements télécoms – qui étaient nombreux à avoir une branche très puissante

de construction de téléphones mobiles au début des années 2000 – ont tous renoncé. Alcatel mais aussi Nokia ont jeté l'éponge. Motorola a cédé ses téléphones à Google, qui a spectaculairement échoué à intégrer cette activité avant de la revendre au chinois Lenovo en enregistrant une colossale perte au passage. Même Ericsson, qui a voulu résister jusqu'au bout grâce à une ambitieuse joint-venture avec Sony, a fini par renoncer. En réalité, aucun de ces groupes n'a su gérer le virage brusque de l'arrivée des smartphones, après qu'Apple a dévoilé l'iPhone en 2007. Il en ira de même d'un spécialiste comme Blackberry, dont les téléphones à clavier physique étaient un quasi-marqueur social avant 2010 avant de disparaître de la circulation en un temps record.

En un sens, Huawei a eu la chance d'arriver tard sur le marché. Le premier téléphone de la marque n'est sorti de ses usines qu'en 2004. À l'inverse des Alcatel, Nokia ou Ericsson, le groupe n'avait pas de vache à lait à protéger. À l'arrivée du smartphone, Huawei a pu embrasser le nouveau format sans état d'âme. Rapidement, le Chinois rejoint les rangs des très nombreux fabricants qui misent sur Android, le système d'exploitation racheté par Google pour faire pièce à l'univers fermé d'Apple. Pour écouler ses produits, il n'hésite pas à les fabriquer en marque blanche pour les grands opérateurs – il a ses entrées dans les états-majors. Son premier appareil à être proposé sur le marché français, l'Ascend P1 en 2012, est à l'époque le plus fin du marché mais ne coûte que 300 euros – deux fois moins cher qu'un iPhone.

Pourtant, Huawei n'a aucune intention de se cantonner à l'entrée et au milieu de gamme. « Il est facile de vendre énormément d'unités à bas prix. Ce que nous voulons, avant tout, c'est aller davantage vers le premium[10] », répète Richard Yu, le patron de la branche Smartphones de Huawei. Cette ambition est salvatrice. Dans la

seconde moitié des années 2010, la montée en puissance d'une multitude d'acteurs chinois – Oppo, Vivo, Xiaomi, TCL, Wiko… – va éreinter les quelques acteurs historiques du milieu de gamme comme le Sud-Coréen LG ou le Japonais Sony, incapables de tenir la dragée haute technologiquement aux deux seigneurs du marché – Samsung et Apple – ou de concurrencer la structure de coût des nouveaux venus. Huawei va s'échapper de ce piège par le haut. Lui a les ressources financières et les équipes de recherche pour aller rivaliser avec les deux grands.

Huawei bénéficie notamment d'un avantage méconnu mais fondamental : sa filiale HiSilicon, que Ren Zhengfei décrit comme « une armée d'assistance qui suit les pas de l'armée principale[11] ». Elle se consacre entièrement à la conception de puces électroniques, qui sont non seulement l'élément le plus cher (après l'écran) d'un smartphone, mais surtout le plus déterminant dans ses performances. On peut compter sur les doigts d'une main les acteurs capables de concevoir des SoC[*1], les petits carrés de silicium qui font des téléphones mobiles actuels des monstres de calcul. L'industrie s'alimente essentiellement pour le haut de gamme chez l'Américain Qualcomm, dont SnapDragon a longtemps été la référence du secteur ; et pour la moyenne gamme, chez le Taïwanais Mediatek. En dehors de ces deux fournisseurs spécialisés, il n'y a guère qu'Apple à avoir très tôt conçu ses propres SoC (dont le dernier modèle A14 Bionic équipe le premier iPhone 5G), suivi par Samsung avec ses SoC Exynos… et Huawei avec sa gamme Kirin. Maîtriser ce « cerveau » du téléphone n'est pas qu'un fait d'armes technologique. C'est aussi la possibilité d'ajuster les caractéristiques de ses puces et de ses téléphones pour optimiser la façon dont ils interagissent et ainsi gagner en rapidité, en efficacité énergétique… Pour les géants du mobile, dessiner ses SoC permet également d'aller parfois plus vite

dans l'innovation que des tierces parties. À l'automne 2020, quand Huawei a dévoilé son dernier modèle haut de gamme – le Mate 40 –, une partie de la présentation a été réservée au Kirin 9000, le deuxième processeur mobile au monde – après la puce A14 d'Apple dévoilée quelques semaines plus tôt – à bénéficier d'une finesse de gravure des transistors de 5 nanomètres. Or, plus ces composants sont minuscules, plus il est possible d'en loger sur la surface d'une puce (15 milliards de transistors pour le Kirin 9000) et plus la puissance de calcul est élevée. La capacité de Huawei à concevoir de telles puces, parmi les meilleures du monde, lui permet de se positionner comme un acteur haut de gamme.

Huawei est l'un des rares fabricants de téléphones dont les modèles phares ont largement dépassé la barre symbolique des 1 000 euros. Au-delà de ses processeurs, la firme vante aussi la qualité de ses appareils photo – un des rares arguments différenciants de l'industrie. En plus de multiples caméras et de zooms optiques sans équivalent, le Chinois peut mettre en avant un partenariat prestigieux. En 2016, il a réussi à signer un contrat de cinq ans avec le fleuron allemand de la photographie Leica, dont la pastille rouge orne désormais les smartphones Huawei. De quoi renforcer encore un peu l'image de produit de luxe que Huawei veut donner à sa production. Pour le lancement du Mate 40, la crise sanitaire l'a empêché de monter un show, en privatisant le Grand-Palais à Paris comme par le passé. Mais pas de lancer une déclinaison du téléphone dessinée en partenariat avec le constructeur automobile Porsche à… 2 300 euros. Le produit restera confidentiel, mais sa seule existence dit la puissance acquise par la marque Huawei.

La concurrence éparpillée

Le début du mois de juillet est habituellement agréable dans les Côtes-d'Armor. Avec les vacances scolaires arrivent les estivants. La crème solaire et les maillots de bain sont de sortie. Mais à Lannion, une petite cité de la côte bretonne, en cet été 2020, ce sont les drapeaux et les banderoles que l'on a ressortis des placards. Nokia, le troisième employeur de la ville – avec 800 salariés et autant de familles qui en dépendent –, vient d'annoncer un « plan de sauvegarde de l'emploi » (PSE). Dans la novlangue administrative, l'expression est un malheureux cache-sexe pour des opérations de licenciement massif. À l'échelle de l'Hexagone, ce sont 1 233 emplois qui doivent être supprimés – soit un tiers des effectifs de Nokia France. Le siège de Nozay, en région parisienne, est le plus durement touché. Mais à Lannion, c'est 50 % des effectifs qui sont poussés vers la sortie. Les syndicats n'ont à présent qu'une crainte : que la direction, dans peu de temps, annonce la fermeture pure et simple du site de Lannion, que Nokia vantait encore quelques années plus tôt comme « un centre de compétences mondial dans le domaine de la cybersécurité ». Dans le centre-ville, des manifestations réunissent plusieurs milliers de personnes. Les drapeaux de la CGT et de la CFDT volent au-dessus des pancartes « Nokia Serial Job Killer » ou « Le Covid m'a épargné. Nokia m'a tué ». Mais de nombreux ingénieurs français sont désabusés. Depuis le rachat d'Alcatel-Lucent par Nokia – et le passage du fleuron français des télécoms sous pavillon finlandais – en 2016, c'est le quatrième PSE – soit une moyenne d'un par an. Bien sûr, les politiques dénoncent l'inélégance de Nokia, qui s'était engagé au moment du rachat à maintenir les effectifs pendant deux ans et à gonfler les équipes de R&D françaises de 25 % pour atteindre 2 500 chercheurs. L'horizon de la promesse (jamais tenue selon les syndicats) à peine atteint, le groupe s'empresse de licencier. L'affaire fait tache. D'autant que le ministre de

l'Économie qui a béni l'union en 2016 était un certain Emmanuel Macron…

Les malheurs de Lannion ne sont qu'un symptôme de la crise profonde traversée par les équipementiers télécoms historiques ces vingt dernières années, comme en miroir de la trajectoire météoritique de Huawei. Le succès du groupe chinois n'est d'ailleurs pas étranger à l'effondrement prématuré de certains d'entre eux. Après tout, c'est sur leurs terres et avec leurs clients que Huawei a fait fortune. « Nous n'avons pas pris leurs marchés ; ce sont plutôt eux qui les ont perdus[12] », tranchera Ren Zhengfei dans une interview au *South China Morning Post* en 2020. Quoi qu'il en soit, la débâcle est indéniable et pour partie liée à Huawei. Ainsi, au printemps 2005, le jour où BT dévoile les vainqueurs de son gigantesque appel d'offres pour son projet « 21st Century Network » à 10 milliards de livres sterling, offrant un tremplin inattendu à Huawei en le reconnaissant comme « fournisseur stratégique », c'est la douche froide pour l'équipementier historique britannique Marconi, qui repart les mains vides. BT n'a rien accordé à son partenaire de toujours, un groupe dont les origines remontent à l'établissement au XIXe siècle par le prix Nobel italien Guglielmo Marconi à Chelmsford, dans le nord-est de Londres, de la toute première usine de radios du monde. Aujourd'hui, le bâtiment de brique claire y est encore visible. Mais Marconi n'est plus. À la suite de l'annonce de BT, l'action de Marconi a plongé. Quelques mois plus tard, les actifs de l'équipementier britannique étaient récupérés par Ericsson pour 1,2 milliard de livres sterling.

Marconi, comme Alcatel ou Nortel, n'avait pas attendu 2005 pour entrer dans la tourmente. À bien des égards, leurs ennuis avaient commencé à une époque où personne hors de Chine n'avait réellement entendu parler d'un petit groupe nommé Huawei. La première crise qui ébranlera sérieusement tous ces géants

technologiques de la fin du XXe siècle est l'explosion de la bulle Internet. Entre les investissements hasardeux dans les start-up en pleine folie « dotcom », les pertes énormes liées à des contrats financés en propre et jamais honorés par des jeunes pousses soudain insolvables et le retournement soudain des marchés financiers contre les valeurs technologiques, le tournant du siècle est un cauchemar. Marconi par exemple, qui valait 35 milliards de livres sterling à la veille du krach, verra sa capitalisation divisée par dix ; elle descendra même sous les 200 millions de livres en 2003, en pleine restructuration pour éponger les pertes.

L'analyse des financiers est alors sans appel. Les équipementiers n'ont pas la taille suffisante pour faire les investissements nécessaires et les amortir sur une large base de clients. À partir de 2006, la valse des fusions s'engage frénétiquement. Le français Alcatel, à peine revenu dans le vert après cinq années de pertes, se marie avec l'Américain Lucent. Quelques semaines plus tard, c'est au tour de Nokia de convoler avec la filiale télécoms de l'Allemand Siemens. Le marché s'éclaircit à vue d'œil. Trois ans plus tard, Ericsson récupère ce qui reste du géant canadien Nortel, en faillite après un scandale comptable, tandis que Nokia reprend les activités de réseaux télécoms de Motorola. Après le rachat d'Alcatel-Lucent par Nokia en 2015 – le deal supervisé par Emmanuel Macron et dénoncé par les syndicats –, il ne reste plus que deux équipementiers occidentaux – Nokia et Ericsson –, contre dix moins d'une décennie plus tôt.

Contrairement aux espoirs des financiers, la course à la taille n'a pas été une solution miracle. Bien souvent, les mariages « entre égaux » se sont traduits par des luttes intestines pour le pouvoir et une désorganisation générale. Après la fusion entre Alcatel et Lucent par exemple, outre l'incompatibilité notoire entre le Français Serge Tchuruk et son homologue américaine Patricia Russo, la suppression

des postes « en doublon » aboutit au départ de cadres expérimentés. Trop occupé à laver son linge sale, le Franco-Américain rate le virage de la 3G et entre dans une spirale descendante. Quinze ans plus tard, elle tourne encore, charriant avec elle des centaines de familles d'une petite commune bretonne.

Le principal bénéficiaire de la vague de concentration du secteur est, paradoxalement, Huawei. Alors que ses concurrents sabrent dans leurs effectifs, lui en profite pour appâter leurs meilleurs éléments. Ainsi, le docteur Wen Tong, patron de la recherche sur les réseaux chez Nortel, est débauché par Huawei après la débâcle de l'équipementier canadien. Ce scientifique – véritable pionnier des réseaux mobiles avec plus de 400 brevets à son crédit et des récompenses en pagaille – travaille toujours à Ottawa. Mais sur sa carte de visite s'affiche désormais « Head of Huawei wireless research ». Ces dernières années, ses travaux ont largement porté sur l'application aux réseaux mobiles du Polar Code, une méthode d'encodage révolutionnaire proposée par un professeur turc en 2008 pour corriger les erreurs de transmission de données à très haut débit. Le pari était osé. Mais il a payé. L'industrie a décidé en 2016 d'en faire une technologie clé de la 5G. Au plus grand bénéfice – en termes de prestige et de royalties à venir – de Huawei, son principal promoteur.

Alors que ses rivaux sont trop occupés à échafauder des plans de fusion et à en gérer les conséquences houleuses, le groupe chinois engrange aussi contrats et parts de marché. Bien que la presse économique lui prête parfois l'intention de racheter tel ou tel acteur, Huawei n'en fait rien. Dans son rapport annuel de 2006, il a indiqué sa philosophie : « La taille n'est pas un facteur absolu de succès. » Il préfère tout miser sur sa croissance organique et l'optimisation de ses propres activités. Parmi les grands équipementiers télécoms d'alors,

un seul a les mêmes réticences que le groupe de Shenzhen. Il s'agit de Cisco, dont l'emblématique patron John Chambers déclare même à l'annonce de la fusion Alcatel-Lucent : « Il est extrêmement peu probable que nous nous lancions dans une grande acquisition. À mon sens, la plupart d'entre elles échouent[13]. » De fait, Cisco n'a pas connu le sort malheureux d'Alcatel. Mais, s'étant toujours cantonné aux équipements de réseaux fixes sans jamais mettre le pied dans le mobile, il n'a pas non plus prospéré comme Huawei.

Qu'aurait-on pu faire différemment ? La question taraude les Américains notamment. Des géants nord-américains d'il y a vingt ans – Motorola, Nortel, Lucent et Cisco –, il ne reste que le dernier. Pire, à l'heure de la 5G, aucune entreprise américaine n'est en mesure de fournir de technologies mobiles de classe mondiale. Les fatalistes diront que c'était inévitable. Mais des voix plus critiques s'interrogent ouvertement sur les conditions dans lesquelles Huawei est ainsi parvenu au sommet. En grattant le vernis du succès, c'est une entreprise vraiment particulière qui apparaît très vite.

---

*1. SoC : System on Chip embarquant généralement un processeur, composé de plusieurs cœurs, un calculateur graphique et souvent un modem et d'autres puces spécialisées dans le traitement d'image.

CHAPITRE III

Un groupe pas comme les autres

Les victoires éclatantes du champion chinois des télécoms sont-elles truquées ? Sa culture interne spartiate mais aussi les conditions extraordinaires de son expansion internationale alimentent en tout cas les critiques – d'aucuns diront les jalousies. Qu'il s'agisse de son management, de ses finances ou de sa diplomatie, Huawei joue sa partition avec brio, mais avec des règles bien à lui.

« 996 »

16 mars 2020, 20 heures. Emmanuel Macron prend la parole à la télévision. Le président annonce le confinement, une mesure sans précédent dans l'histoire du pays. Dès le lendemain, des dizaines de millions de Français s'enferment chez eux pour ralentir la propagation du coronavirus. La méthode, expérimentée en Chine ou en Italie peu de temps auparavant, a montré son efficacité sanitaire. Mais elle a des effets de bord inattendus, notamment pour les télécoms. Soudain amenés à télétravailler, à faire l'école sur Internet et même à prendre l'apéritif en visioconférence, les consommateurs

font exploser la bande passante. Et, partout sur le territoire, les opérateurs se démènent pour renforcer les réseaux en urgence. Huawei, un des principaux fournisseurs de Bouygues Telecom et de SFR, est sur le pont. Jamal El Ghoulti, responsable sécurité et qualité pour la filiale française du groupe chinois, est mobilisé comme jamais. La première semaine du confinement, le jeune homme parcourt 1 538 km à travers la Bretagne pour modifier les paramétrages des antennes mobiles et augmenter la capacité du réseau. « J'embarque des produits secs pour manger. Et je prévois la possibilité de dormir dans la voiture[1] », explique-t-il aux *Échos*.

Ce genre d'abnégation n'est pas rare chez Huawei. Elle est même largement encouragée et mise en avant par le groupe. Au début de la crise sanitaire, alors que la Chine et le monde connaissent encore très mal le virus, ses vecteurs de transmission ou sa létalité, les équipes de Huawei sont envoyées à Wuhan, la désormais célèbre capitale de la province du Hubei. En un temps record, deux hôpitaux de la ville sont équipés d'un réseau 5G flambant neuf. L'occasion est parfaite de montrer les capacités de la nouvelle technologie. Les portes de la ville ont été fermées, mais les ondes radio, elles, peuvent continuer de circuler et permettre aux autorités sanitaires de la métropole de partager avec la communauté scientifique les images et analyses du foyer épidémique.

Cette forme de mépris du danger est institutionnalisée. « Huawei est une entreprise qui ne fuit pas face aux catastrophes[2] », professe Ren Zhengfei, qui rappelle souvent à ses interlocuteurs l'épisode tragique de Fukushima. Le 11 mars 2011, le plus important séisme mesuré au Japon secoue le nord-est de l'archipel. Il est 3 heures de l'après-midi, les maisons vacillent. Mais le pire est à venir. Moins d'une heure plus tard, une gigantesque vague de plusieurs dizaines de mètres de haut déferle sur la côte. Elle va provoquer la mort de

15 000 personnes, mettre des centaines de milliers d'autres sur les routes et causer la deuxième plus grave catastrophe nucléaire de l'histoire après Tchernobyl. Dans ce no man's land inondé et irradié, rares sont les téméraires à s'aventurer dans les jours qui suivent le drame. Risquant leur vie, des employés de Huawei sont pourtant accourus. En deux semaines, ils restaureront 680 sites mobiles. Meng Wanzhou, la directrice financière de Huawei – et la propre fille de Ren Zhengfei –, prend elle-même un vol à Hong Kong pour se rendre au Japon. Ils ne sont que deux passagers à bord de l'avion.

Il faut dire que les convictions du patron sont clairement affichées : « Seuls ceux qui ont été sur un champ de bataille, qui ont tiré les balles et qui ont été blessés au combat pourront être promus, explique-t-il. Chez Huawei, si on n'a pas travaillé dans les endroits les plus éprouvants, on ne pourra pas faire partie de la direction[3]. » Il n'est pas rare pour les jeunes cadres ambitieux d'être affectés dans des pays en guerre. C'est par exemple le cas de Linda Han. Jeune trentenaire aux cheveux courts et à la mise stricte toujours impeccable, elle a pris à l'été 2019 les commandes de la filiale française, dont elle parle remarquablement bien la langue pour avoir passé les dix années précédentes en Afrique francophone, d'abord au Burkina-Faso, puis en Côte d'Ivoire, en pleine crise post-électorale. Les balles fusent dans la capitale, entre les factions fidèles à l'ancien président Laurent Gbagbo et celles de son rival, Alassane Ouattara. « Il y avait des coupures d'électricité, et les réseaux de télécommunications tombaient en panne. Nous avons traversé l'un des ponts d'Abidjan, escortés par l'armée française, pour arriver au central téléphonique et rétablir le signal, raconte-t-elle aux *Échos*. Huawei est le seul équipementier à être resté sur place. Je suis très fière de cette histoire[4]. »

Les méthodes managériales pour le moins exigeantes du groupe sont devenues célèbres. Le fait par exemple que, dans la première phase de croissance du groupe de Shenzhen, les bureaux des ingénieurs étaient tous munis d'un petit matelas à déplier pour pouvoir dormir quelques heures pendant les nombreux coups de chaud, est entré dans la légende de Huawei – où l'on parle de « culture du matelas » pour désigner cet acharnement au travail. Un autre terme clé est souvent associé au groupe, en particulier sur Weibo – l'équivalent de Twitter en Chine : « 996 ». Derrière ce chiffre se cache une réalité à faire bondir un syndicaliste : travailler de 9 heures du matin à 9 heures du soir, six jours par semaine. À la décharge de Huawei, de nombreux groupes chinois comme Alibaba sont fréquemment accusés de favoriser le « 996 ». Celui-ci relève moins d'une politique d'entreprise que d'un trait culturel asiatique au sens large dans la valeur sociale accordée à l'effort. Ren Zhengfei a par ailleurs officiellement démenti que le « 996 » avait cours chez Huawei. Mais cela n'empêche que l'histoire du groupe est émaillée de pratiques curieuses à l'œil occidental, comme les campagnes de démission de masse ou de réduction de salaires volontaires organisées dans les années 1990 et 2000. Ainsi que le décrit Yang Shaolong dans son ouvrage sur le groupe, ce sont les employés qui sont encouragés à se sacrifier collectivement pour le bien de Huawei : « L'objectif de ces campagnes n'est pas de persécuter ses employés, il est de faire progresser et d'améliorer la gestion de Huawei en instillant un sentiment de crise artificiel[5]. »

La culture loup

Au cours de trois décennies, Ren Zhengfei, fasciné par les méthodes de gestion américaines, aura fait intervenir chez Huawei pléthore de cabinets étrangers, notamment IBM. De son propre aveu, ce sont ainsi des dizaines de milliards de dollars que Huawei a dépensés en frais de conseils. Mais le groupe n'a jamais renoncé pour autant à ses spécificités, résumées sous l'appellation « culture loup ». Le terme provoque une certaine incompréhension à l'étranger, où le grand prédateur renvoie à une imagerie populaire négative. Mais pour Huawei, les loups ont trois caractéristiques essentielles : ils ont une grande sensibilité, sont persévérants et travaillent en meute. Huawei est la meute. Et ses salariés sont tenus de lui donner le meilleur d'eux-mêmes, comme à la guerre. « Nous disons que s'il faut mourir, mourons sur le champ de bataille, assume Ren Zhengfei. Même si l'on ne peut pas soutenir le combat principal, on peut toujours cuisiner pour l'équipe. Vous serez récompensés quand l'équipe réussit, peu importe le rôle que vous jouez[6]. »

L'ambiance martiale est assumée. Ceux qui ne supportent pas peuvent quitter les rangs. « Je pense qu'ils sont assez nombreux à être effrayés par ce style, reconnaît lui-même Ren Zhengfei. Et j'en ai pour preuve les 160 000 personnes qui ont choisi de quitter Huawei depuis toutes ces années[7]. » Ceux qui restent savent à quoi s'en tenir. Les mots d'ordre sont : obéissance, engagement et… humilité. Plutôt que de se rengorger de ses succès, chaque employé est invité à faire publiquement et fréquemment son autocritique – à commencer par le fondateur, dont la liste des « dix crimes » est publiée sur la communauté virtuelle interne, Xin Sheng, et accessible à tous.

Si ces confessions publiques personnelles sont encouragées, il est en revanche inconsidéré de faire des critiques plus générales. En novembre 2019, un employé des ressources humaines se plaint sur Xin Sheng dans une lettre qui deviendra virale sur les réseaux sociaux

chinois. « Le nombre d'heures supplémentaires moyen parmi les équipes de recherche du Huawei 2012 lab a atteint 57 heures… mais la loi nationale sur le travail fixe le maximum à 36 heures, écrit Hu Ling. La principale mission des employés seniors des ressources humaines semble être d'aider l'entreprise à s'exonérer de toute responsabilité quand les gens font un burn-out[8]. » Face à la bronca, Ren Zhengfei répond lui-même à la missive, en demandant que les débats internes ne s'invitent pas sur la place publique. Hu Ling démissionnera.

Ce besoin de maintenir ses troupes sous un contrôle étroit peut avoir des conséquences encore plus inquiétantes. Peu après l'affaire de Hu Ling, un autre cas attire l'attention des médias du monde entier, celui de Li Hongyuan, un ancien salarié emprisonné pendant plus de huit mois pour extorsion avant d'être relâché faute de preuves[9]. Licencié, l'infortuné avait eu le malheur de vouloir négocier une indemnité. L'affaire provoque une vague de colère en Chine. Les censeurs tentent bien d'effacer de la Toile les articles et messages qui s'y rapportent. Mais les internautes chinois ont l'habitude de ce jeu du chat et de la souris. Et de nombreux commentaires se contentent d'afficher « 251 » ou « 404 » sur Weibo. Le premier chiffre se réfère au nombre de jours de détention de Li Hongyuan ; le second, au message d'erreur qui s'affiche sur Internet quand une page est introuvable.

Dans la foulée, plusieurs autres cas d'emprisonnement d'anciens salariés sont mis au jour. L'un d'eux, Zeng Meng, dînait paisiblement en famille lors de vacances en Thaïlande lorsque la police chinoise est venue l'interpeller. Extradé en Chine, il est inculpé pour « violation de secrets commerciaux » et incarcéré quatre mois à Shenzhen, pendant lesquels il ne quittera pas la petite cellule où il dort à même le sol avec plusieurs dizaines de codétenus. Les charges seront transformées

en « fraude », avant qu'il ne soit libéré sous caution. L'affaire est embarrassante en soi. Elle le deviendra encore plus un an plus tard. Fin avril 2020, le *New York Times* révèle une coïncidence troublante. Quelques jours avant d'être arrêtés sans ménagement par la police, Zeng Meng, Li Hongyuan et trois autres anciens de Huawei également mis sous les barreaux avaient tous échangé sur un groupe WeChat – la messagerie privée la plus populaire de Chine. Les cinq employés mécontents abordaient notamment un sujet brûlant : les activités commerciales de Huawei en Iran. Selon le grand quotidien américain, la police aurait clairement indiqué aux deux hommes qu'ils avaient franchi une ligne rouge[10]…

Mystère Ren

Plus que les pratiques martiales de Huawei, c'est justement sa proximité supposée avec l'appareil sécuritaire chinois qui fait tiquer les observateurs étrangers, et en particulier la personnalité atypique de son fondateur et quasi-gourou, Ren Zhengfei. Comment expliquer autrement qu'un homme sans expérience et sans financement puisse créer une entreprise et en faire le numéro 1 des télécoms en moins de trente ans ? Après tout, le personnage n'est-il pas lui-même un ancien militaire ? Parmi ses lectures favorites, on trouve le traité de stratégie *De la guerre* du général prussien Clausewitz. Au siège du groupe, il a fait accrocher des grandes huiles représentant des épisodes de l'épopée napoléonienne. Et les maximes militaires reviennent sans arrêt dans ses prises de parole. Ren Zhengfei a beau avoir quitté l'Armée populaire de libération (APL) il y a bientôt quarante ans, rien n'y fait. Ses détracteurs continuent de voir en lui un agent masqué de la puissante APL.

La faute originelle, c'est d'avoir effectivement rejoint les rangs de l'armée chinoise en 1974 et d'y avoir œuvré pendant près de dix ans. Mais à cette aune, combien d'entreprises américaines sont dirigées par d'anciens haut gradés ? Et combien d'autres offrent des sièges d'administrateur à d'anciens de la CIA ou de la NSA ? Sans compter que rejoindre les rangs de l'armée au début des années 1970, alors que la révolution culturelle bat son plein, est le lot commun de centaines de milliers de jeunes hommes et l'un des rares moyens de s'extraire de la misère.

L'histoire personnelle de Ren Zhengfei, telle que la retracent les services de communication de Huawei, est à ce titre exemplaire. Loin d'être le rejeton d'un prince rouge, le magnat des télécoms est un self-made-man comme la mythologie américaine les rêve. Né en 1944 dans une famille nombreuse de la province montagneuse et reculée du Ghizou, le chef a une enfance surtout marquée par la faim et le froid. Sa seule chance est d'avoir deux parents enseignants – ce qui leur vaut des ennuis dans la tourmente maoïste mais qui permet au jeune Ren Zhengfei de faire des études supérieures. Il sortira diplômé en ingénierie civile de l'université de Chongqing, avant d'entrer dans les unités scientifiques de l'armée, qui l'envoient au fin fond de la Chine rurale monter une usine de fibres synthétiques, avec des machines françaises signées Technip.

Mais comment cet officier de second rang, qui n'aurait jamais dépassé le grade de chef d'escadron selon ses dires, a-t-il pu être invité au rassemblement politique le plus prestigieux de Chine, le Congrès national du parti, en 1982 ? Les soupçonneux y voient la preuve que Ren Zhengfei entretient très tôt des liens bien plus étroits que ce qu'il avoue avec les élites de la Chine communiste. L'intéressé explique, lui, qu'ayant inventé un appareil sans équivalent à l'époque pour contrôler la qualité de la production de son usine, il est promu

délégué de l'APL pour assister à la Conférence nationale des sciences, puis invité au Congrès national du parti en guise de remerciement.

Quant à son adhésion au parti communiste à la même époque, elle fait hausser les épaules au patron de Huawei. « Si vous n'êtes pas membre du parti, vous ne pouvez même pas devenir chef de l'équipe de cuisine[11] », explique-t-il en 2019. Rétrospectivement, Ren Zhengfei a eu sa carte plutôt tard. Alors que sa première femme, Meng Jun, qu'il décrit lui-même comme « un caractère bien trempé[12] », est le commissaire politique des 300 000 gardes rouges de Chongqing, le mouvement paramilitaire de volontaires dévoués à Mao, le jeune homme est handicapé par ses antécédents familiaux. « Mon père a été traité de "personne de tendance capitaliste", explique Ren Zhengfei. […] Le contrôle strict du parti communiste l'empêchait de rétablir sa réputation pendant dix ans, je ne pouvais donc pas rejoindre le parti[13]. »

Aujourd'hui encore, le patron minimise en permanence ses connexions politiques, plaisante sur le fait qu'il n'a pas le numéro de téléphone des dirigeants ou qu'il ne se souvient pas de la dernière fois qu'il a rencontré un officiel. Il est pourtant évident qu'au cours du développement international de Huawei, le patron – comme n'importe lequel de ses pairs – a participé à moult voyages d'État, au sein des inévitables délégations économiques qui espèrent signer des contrats dans le sillage des politiques. Et les autorités chinoises elles-mêmes ne peuvent pas ignorer cet homme d'affaires hors du commun.

Ce n'est pas qu'il soit si riche. Dans un pays qui compte plus de 2 000 milliardaires en dollars, la fortune de Ren Zhengfei, estimée à 3 milliards, n'a rien d'exceptionnel. Il n'est même pas dans la liste des 250 personnes les plus fortunées de Chine. Le patron de Huawei est très loin de peser autant que Jack Ma, le fondateur d'Alibaba et ses

59 milliards de dollars – l'homme le plus riche de Chine –, ou même que Lei Jun, le fondateur de Xiaomi, avec ses 25 milliards.

En revanche, il dispose d'une aura extraordinaire dans son pays. Il est le patriarche de la tech chinoise, celui qui a donné parmi les premiers un sentiment de supériorité et de fierté à ses compatriotes. Chez Huawei, Ren Zhengfei bénéficie d'un quasi-culte de la personnalité. Ses citations ornent les murs des bureaux. Ses mémos sont envoyés régulièrement à tous les salariés du groupe. Et les retranscriptions de ses entretiens et ses points de vue sont omniprésents sur le forum interne Xin Sheng.

Cette dévotion est aussi due à la singularité du personnage. Très discret, obsédé par le travail et jamais avare d'un sacrifice personnel, c'est un général qui sait parler au commun de la troupe. Jusqu'au début des années 2000, alors que son groupe explose, il ne possède toujours pas son propre appartement, car tous les gains sont réinvestis en R&D. Et l'exigence qu'il impose à ses employés, il se l'applique à lui-même. « Je me suis rendu personnellement au camp de base du mont Everest situé à 5 200 m d'altitude pour voir nos stations de base installées là-bas, explique-t-il. On m'a dit de ne pas y aller. J'ai dit : "Pourquoi je ne peux pas y aller ?" Si j'ai peur pour ma peau en grimpant sur cette hauteur, je n'aurai donc pas le droit de demander aux ingénieurs de venir installer les équipements ici[14]. »

L'armure d'austérité de Ren Zhengfei a une faille. Elle s'appelle Annabel Yao, et c'est la deuxième fille et dernière des trois enfants du magnat des télécoms. En 2018, la jeune héritière apparaît sur les escaliers du palace Shangri-La à Paris pour le Bal des débutantes, un des événements caritatifs les plus selects de la planète qui réunit chaque année vingt jeunes femmes – baronnes, princesses et autres héritières d'empires industriels – habillées par les plus grandes maisons de couture. Pour *Paris Match*, qui consacre alors un portrait à

cette « fille du Ciel dans la ville Lumière[15] », l'étudiante en informatique à Harvard a réussi à faire poser son père avec elle dans un des salons du palais de réception de Huawei, à Shenzhen – un exploit. La jeune *socialite*, fan d'Instagram autant que de ballet classique, contrebalance l'image du septuagénaire reclus. Elle assume son appartenance à une élite mondialisée et arbore souvent… un iPhone.

Ren Zhengfei n'y trouve rien à redire. Lui-même est fan de Steve Jobs. Quand le fondateur d'Apple est décédé, Annabel Yao a même organisé une séance de deuil d'une minute en famille. Son père refuse de se mettre sur le même piédestal. Lors d'une interview au *South China Morning Post*, il se compare plutôt à une idole en argile : « Sans elle, le temple aurait l'air vide, mais en vérité, l'idole ne fait pas vraiment quoi que ce soit. […] Un jour, je disparaîtrai[16]. » La question sera ce jour-là de savoir si, sans cet ex-militaire mystérieux qui fascine ses troupes autant qu'il nourrit les soupçons de ses adversaires, Huawei aura moins de mal à convaincre de son indépendance.

Leçons de séduction

Nous sommes en août 2012, dans une chambre d'hôtel de Canberra, en Australie. Ren Zhengfei allume la télévision. La première image qui s'affiche à l'écran est celle d'un match de rugby, opposant le club local des Raiders aux Panthers de Penrith. Dans ce classico austral, c'est Canberra qui s'impose cette fois, 20 à 10. Est-ce pour saluer la visite exceptionnelle de celui qui vient d'accepter d'être son principal sponsor ? En tout cas, le lendemain, c'est un Ren Zhengfei tout sourire qui rencontre les joueurs. Il pose pour les

photographes, maillot vert à la main, floqué à son nom, « Ren Z. F. », et bardé du numéro 1, sous le logo rouge du groupe chinois. C'est le premier partenariat sportif de Huawei. Pendant près d'une décennie, le groupe mettra des millions sur la table pour voir son logo en évidence sur le torse des Raiders. Une opération de promotion comme une autre ? Sans doute, si ce n'est que le club n'est pas le meilleur de la National Rugby League australienne. Mais il a l'avantage indéniable de jouer dans la capitale administrative du pays. Le stade est à un quart d'heure en voiture du Parlement et de nombreux députés comptent parmi ses habitués.

La formule du partenariat sportif séduit en tout cas Huawei. Pour bâtir sa notoriété, le groupe va multiplier les contrats prestigieux. Et les plus chers, donc. Les plus grands clubs de football sont ravis de voir débarquer ce nouveau Crésus asiatique, qui dépense sans compter pour s'acheter de la visibilité. Huawei sera ainsi le partenaire du Milan AC, d'Arsenal, de l'Atletico Madrid, de Schalke 04, de l'Ajax Amsterdam, du Benfica Lisbonne, du Paris-Saint-Germain… Outre qu'il amène sa technologie pour doper la connectivité dans les stades ou pour truffer les espaces d'entraînement des joueurs de matériel high-tech afin de suivre leurs performances, Huawei se voit ainsi associé à une image de puissance et de prestige qui est loin d'être la norme pour les marques chinoises en Europe au début des années 2010.

Continuant de faire flamber le chéquier, le groupe s'offre aussi les services de stars du ballon rond pour devenir les « ambassadeurs » de la marque. Il y a le Colombien James Rodriguez ou le Chilien Alexis Sanchez, qui font la retape des produits au lotus en Amérique du Sud. Il y a surtout Leo Messi, le prodige du FC Barcelone, qui abandonne Samsung pour signer en 2016 avec Huawei pour trois saisons, moyennant – à en croire la presse sportive espagnole[17] – la

bagatelle de 15 millions d'euros. Le symbole est fort. Le meilleur joueur du monde qui opte pour un nouveau fournisseur… est-ce un signe que la couronne de roi des smartphones est sur le point de changer de main ? Question symboles, en tout cas, Huawei est servi : en 2017, c'est le chouchou des Français, Antoine Griezmann, qui devient à son tour l'égérie de la marque. Un joli coup, puisque cela permet à Huawei d'accompagner « Grizou » à Moscou, un certain 15 juillet 2018, le jour où l'équipe de France de football décroche une deuxième étoile à son maillot. Le résultat est à la hauteur de la débauche de moyens. Quasi inconnue quelques années plus tôt, Huawei s'invite dès 2014 dans le top 100 des meilleures marques mondiales établi par Interbrand[18]. Le lotus rouge n'en est pas sorti depuis. En 2020, il figure en 80e place, juste derrière Ferrari mais devant Dior.

Des lobbyistes de choc

En plus des sportifs, des stars et des paillettes, Huawei mène une politique de recrutement plus discrète mais tout aussi essentielle. Celle qui doit lui permettre, non pas de se faire connaître du grand public, mais de gagner ses entrées dans les cercles de pouvoir. En Australie, non content de sponsoriser le club de rugby préféré des députés, Huawei recrute plusieurs politiques, dont un ancien ministre des Affaires étrangères, pour siéger au conseil d'administration de sa filiale, présidée par un amiral de la marine australienne.

En 2011, dans sa pêche secrète aux personnalités de choix, Huawei ferre un très gros poisson. John Suffolk vient de passer sept années comme directeur de l'informatique et de la sécurité du gouvernement britannique. C'est un technicien, auteur d'un rapport

sur la cybersécurité au moment où la Chambre des communes lance une enquête sur l'attribution du fabuleux marché de BT à 10 milliards de livres sterling, dont Huawei est ressorti grand gagnant en 2005. C'est aussi un très haut fonctionnaire, qui connaît extrêmement bien les arcanes de Westminster. Or le Royaume-Uni est devenu la tête de pont du groupe chinois en Occident. Huawei n'hésite pas longtemps avant de confier à John Suffolk le poste de responsable mondial de la cybersécurité.

Peu de temps après, autre prise marquante : Huawei recrute Andy Purdy pour être le relais de John Suffolk sur le marché américain. Celui où il n'arrive pas à percer. Celui donc où il a le plus à cœur de séduire les politiques en montrant patte blanche. De ce point de vue, Andy Purdy affiche un pedigree au moins aussi valable que celui de John Suffolk. Il a longtemps été un des premiers responsables de la cybersécurité de l'administration américaine, au point d'être à l'origine de la « stratégie nationale pour sécuriser le cyberespace » dévoilée en 2003 par le président George W. Bush, dont il était le conseiller à la Maison-Blanche… Tout au long des années 2000, Huawei débauche aussi des cadres de l'industrie – les directeurs techniques de Nortel, John Roese, ou de BT, Matt Bross, l'homme qui supervisait le programme à 10 milliards de livres « 21st Century Network », rejoignent ses rangs.

En France, c'est sur François Quentin que Huawei s'est longtemps reposé pour faire du charme aux opérateurs, mais aussi à l'Élysée et à Matignon. Ex-directeur de la division aéronautique du groupe Thales – un temps pressenti par la famille Dassault pour prendre la tête du groupe d'armement –, l'ingénieur télécoms déclare en 2010 aux *Échos* avoir accepté le poste de président de Huawei France « pour que justement cessent ces questions non pertinentes[19] » sur les liens de Huawei avec le pouvoir chinois ou les risques d'espionnage. À son

départ en 2019, ce sera un ancien ministre, le maire de Valenciennes, Jean-Louis Borloo, déjà présent depuis plusieurs années au conseil d'administration de la filiale, qui en assurera brièvement la présidence, avant de passer la main à Jacques Biot, l'ex-patron de l'École polytechnique, qui préside un *board* où pointe un autre ancien du gouvernement français, le socialiste Jean-Marie Le Guen.

Quel que soit le bord politique des recrues de Huawei, leur tâche est la même. Mettre leur carnet d'adresses au service du groupe chinois. À l'occasion, ils en assurent la défense. Ainsi en 2012, lorsque le sénateur Jean-Marie Bockel fait approuver par la Commission des affaires étrangères et des forces armées du Sénat son rapport encourageant l'interdiction en Europe des routeurs et équipements de cœur de réseaux chinois, François Quentin dénonce publiquement « un tissu d'allégations sans preuve, qui reprend les rumeurs sans fondement qui circulent sur Internet depuis dix ans[20] ».

Huawei peut également compter sur ces vigies aux longues antennes pour se repérer dans les méandres de la politique locale. Identifier les acteurs favorables au renforcement des liens avec Pékin, par exemple, est très utile pour le fleuron technologique chinois. Aux rangs de ces sinophiles, on compte bien sûr l'ancien Premier ministre Jean-Pierre Raffarin, mais aussi des acteurs plus discrets et au moins aussi efficaces comme Emmanuel Lenain. L'actuel ambassadeur de France en Inde a longtemps été consul général à Shanghai avant de rejoindre Édouard Philippe à Matignon comme conseiller diplomatique entre 2017 et 2019. Fervent partisan d'une coopération renforcée avec Pékin, il est l'un des cofondateurs de la France China Foundation. Cette structure organise notamment les Young Leaders[21], un programme d'échange annuel entre quelques dizaines de jeunes profils prometteurs des deux pays. La France China Foundation a pu emmener en Chine, en tant que Young Leaders, plusieurs députés, au

moins cinq futurs ministres et un futur Premier ministre (Édouard Philippe). C'est dire la force de ce réseau d'influence. Chaque année, le club très élitiste se réunit également pour une soirée de gala. Le 16 mai 2018, celle-ci se tenait dans la galerie des Batailles du château de Versailles, louée pour l'occasion pour la coquette somme de 160 000 euros[22]. Dîner gastronomique, concert du violoniste Renaud Capuçon et du pianiste Xue Yingjia, feu d'artifice dans les jardins… Sur une des photos de cette soirée enchanteresse, Emmanuel Lenain pose avec Jean-Pierre Raffarin[23]. De part et d'autre de Ken Hu, l'un des trois vice-présidents tournants de Huawei.

En plus de travailler son entregent, Huawei n'hésite pas à pratiquer la politique du portefeuille et à promettre aux politiques les investissements dont ils ont électoralement tant besoin. En 2012, Ren Zhengfei est à Downing Street pour une rencontre avec le Premier ministre britannique David Cameron. Le patron annonce qu'il va débourser 2 milliards de dollars Outre-Manche et recruter 700 personnes pour doubler ses effectifs en cinq ans. Deux ans plus tard, rebelote à Matignon, où le même Ren Zhengfei s'assoit avec Manuel Valls pendant 45 minutes et lui présente un plan d'investissement de 1,5 milliard d'euros, avec à la clé 650 salariés supplémentaires d'ici à 2018 et, à terme, 200 chercheurs. Le genre de discours qu'un Premier ministre arrivé quelques mois plus tôt aux affaires aime entendre. Et qui peut apaiser certaines réticences. Pour les faire disparaître, Huawei est prêt à aller encore plus loin.

The Cell

C'est un bâtiment récent de deux étages, en brique rouge et au toit d'ardoises, semblable à ses voisins avec lesquels il partage un

parking de 80 places. On dirait un modeste site de bureau de banlieue. Le centre-ville de Banbury, petite commune de 50 000 âmes voisine d'Oxford, n'est qu'à 2 km. Mais le rond-point qui jouxte le site donne d'un côté sur les champs, de l'autre sur un entrepôt d'Amazon. Sur un des bâtiments voisins, on lit le sigle d'une PME de cartographie maritime, sur un autre, celui d'une banque suédoise. Absolument rien ne permet de penser qu'ici est logé un des services critiques des renseignements britanniques. Si ce n'est peut-être une longue banderole blanche sur le flanc des bâtiments, vaguement cachée des regards, où l'on peut lire : « Cyber Security Evaluation Center », à côté du logo rouge de Huawei.

Bienvenue au Centre d'évaluation en cybersécurité Huawei, ou plutôt, comme les espions britanniques l'appellent dans leur jargon, « The Cell ». Cet organisme est unique au monde. Depuis 2010, dans le cadre d'un arrangement avec les autorités, le groupe chinois permet aux cyber-experts de Sa Gracieuse Majesté de démonter pièce par pièce chacun de ses équipements qui a vocation à être installé sur le territoire britannique. Ils ont également accès au précieux code source – l'intégralité des millions de lignes de commandes qui forment le logiciel des antennes mobiles ou des routeurs du constructeur chinois[24]. Ils sont ainsi une quarantaine à traquer la moindre faille dans les produits fournis par Huawei. Et l'ensemble de l'opération est financée… par le groupe de Shenzhen, trop heureux d'avoir une occasion de montrer au monde que ses équipements sont fiables et exempts de tout composant matériel ou logiciel qui permettrait à Pékin d'espionner ou de perturber les réseaux. Le GCHQ – le service de renseignements électroniques de la Couronne – ne voit pas de problème à ce que ses limiers soient rémunérés directement par le groupe sur lequel ils enquêtent. Aucun n'est en relation directe avec le siège à Shenzhen, sauf le directeur de The

Cell, un ancien directeur adjoint du GCHQ avec des dizaines d'années d'expérience.

Chaque année, The Cell produit un rapport d'expertise à destination des autorités, pour juger du degré de risque à intégrer les équipements Huawei dans les réseaux britanniques. Pour le groupe chinois, le jeu en vaut la chandelle. S'il passe la barre des espions britanniques, le rapport peut lui servir de blanc-seing à faire valoir dans tous les pays du monde où l'on vient resservir la vieille rengaine du risque d'espionnage. Pour les autorités britanniques, c'est un moyen de se rattraper. Lorsque BT, en 2005, a décidé de confier une partie de son nouveau réseau fixe ultramoderne à Huawei, le gouvernement n'a pas été informé. C'est ce qui ressort d'un rapport parlementaire[25] sur l'épisode, livré sept ans plus tard, dans lequel les députés déplorent que si BT avait bien notifié certains officiels dès 2003 de l'intérêt de Huawei pour son appel d'offres, ceux-ci ont d'abord estimé qu'il était de toute façon légalement impossible de faire quoi que ce soit et que bloquer Huawei aurait des « conséquences potentielles trop importantes en termes de commerce, de finance et de diplomatie ». Aucun ministre n'a donc été mis dans la boucle. Et les députés de regretter, bien plus tard, que le gouvernement soit « parfois mis dans la position d'essayer de fermer la porte de l'écurie après que le cheval s'est échappé ».

Au NCSC, Ian Levy ne voit pas les choses de cette façon[26]. Selon le directeur technique, ses équipes avaient bien en tête, dès le début du contrat entre Huawei et BT, que la Chine pouvait non seulement exiger de n'importe quel acteur national une obéissance totale, mais qu'elle commettrait des cyberattaques contre le Royaume-Uni à un certain point. Cependant, « aucun attaquant n'est omnipotent et omniscient ; les lois de la physique s'appliquent tout de même à eux », rappelle l'espion, qui estime que les mesures de protection

alors en place – notamment en termes de supervision et de diversification des fournisseurs pour limiter la propagation d'un problème à l'ensemble du réseau – étaient suffisantes. Ce n'est que plus tard, à partir de 2008, quand d'autres opérateurs que BT ont aussi souhaité déployer des équipements Huawei que, pour ne pas dupliquer les mesures imposées à BT, un nouveau système a été imaginé : The Cell. Quoi qu'il en soit, le discours est très clair. Parce qu'il est Chinois, Huawei est contraint à un examen minutieux auquel aucun de ses concurrents occidentaux n'est soumis. Début 2020, le patron de l'Anssi, Guillaume Poupart, ne dit pas autre chose dans une interview aux *Échos* : « Je sais très bien qu'il y a des risques plus forts avec des équipements qui viennent de Chine, donc construits par une entreprise qui est, malgré elle, soumise à des pressions éventuelles venant du gouvernement chinois. […] Je sais qu'un pays membre de l'Union européenne ne va pas faire pression sur Nokia ou Ericsson pour éteindre les réseaux en France. C'est un scénario qu'on ne prend pas en compte[27]. »

Le Royaume-Uni est le seul pays au monde à disposer de The Cell, un centre autonome truffé d'espions payés par Huawei. Mais le groupe n'a cessé de proposer à tous les États qui le souhaitent d'ouvrir des structures pour examiner ses produits. Le 5 mars 2019, au 13 rue Guimard, dans le quartier européen de Bruxelles, non loin du Parlement et du Berlaymont – l'immeuble qui héberge la puissante Commission européenne –, une réception est organisée. Il y a des représentants de l'Union européenne, de la GSMA, du Forum économique mondial, et l'un des trois vice-présidents de Huawei, Ken Hu, venu inaugurer le sixième centre de transparence sur la cybersécurité du groupe – après ceux de Banbury, Bonn, Dubaï, Shenzhen et Toronto. Les murs blancs sont couverts d'écrans et de slogans comme « La 5G est une responsabilité partagée ». Mais les

1 000 m^2 sont plus qu'une vitrine de communication, ils sont aussi ouverts aux clients du groupe et aux tierces parties, invités à « effectuer des tests de sécurité indépendants, justes et objectifs » grâce à la mise à disposition gracieuse de produits, logiciels, documents techniques, outils de mesure et support technique. À son auditoire, Ken Hu assène : « La confiance doit reposer sur des faits, les faits doivent être vérifiables et la vérification doit reposer sur des standards communs. Nous pensons qu'il s'agit d'un modèle efficace pour construire la confiance à l'ère numérique[28]. » Deux ans plus tard, c'est au tour de Rome de se voir promettre la construction d'un centre de transparence sur la cybersécurité. L'ouverture est prévue en septembre 2021. Las, il est déjà certain que cette nouvelle dépense échouera à éteindre toute polémique. D'autant qu'elles ne se limitent pas à des arguments techniques. Les conditions économiques dans lesquelles Huawei s'est développé font aussi grincer bien des dents à l'Ouest.

Des conditions généreuses

En novembre 2000, Ren Zhengfei parcourt le continent africain. Il n'est pas seul. Le patron accompagne le ministre chinois des Affaires étrangères d'alors, Wu Bangguo, dans une vaste tournée diplomatique. Un mois plus tôt s'est tenu à Pékin le premier Forum économique Chine-Afrique, un rendez-vous trisannuel entre les dirigeants africains et le gouvernement chinois, qui deviendra vite l'antichambre où se négocient et se signent de mirifiques contrats. Ce début du siècle coïncide avec une offensive économique de grande ampleur, qui verra la Chine devenir en quinze ans le premier investisseur étranger du continent, bâtissant des routes, des ports, des

infrastructures pétrolières… et des réseaux télécoms. C'est pour cela que Ren Zhengfei s'est glissé dans la suite ministérielle. Le patron met notamment à profit les échanges diplomatiques pour négocier ce qui sera bientôt un des plus gros contrats de Huawei, raconte le Jetro – l'Agence du commerce extérieur japonais – dans un rapport publié en 2009 sur la Chine en Afrique[29]. Le Nigeria confiera en 2005 la construction d'un réseau 3G national à l'équipementier de Shenzhen. Le contrat atteint 200 millions de dollars. Mais ce sont ses petites lignes qui intriguent. L'intégralité de la somme a été prêtée au Nigeria par la China Development Bank en 2004, à des taux imbattables, « parfois jusqu'à 1 ou 2 % », écrit le Jetro. À l'époque, la moyenne est de plus de 6 % en Chine. La manœuvre s'apparente à une sacrée subvention, aux frais du contribuable chinois.

L'exemple est loin d'être isolé. Chacun, dans le petit monde des télécoms, a une anecdote sur la façon dont Huawei lui a prétendument chipé un marché en jouant avec ses propres règles du jeu. Travis Russell, le directeur de la cybersécurité d'Oracle – un grand éditeur de logiciels américains qui veut aussi se faire une place sur le marché des télécoms –, raffole particulièrement de deux d'entre elles, qu'il livre début 2019 lors d'une conférence sur la sécurisation des réseaux 5G, organisée par le think tank américain CSIS (Center for Strategic & International Studies)[30]. « Je vais vous raconter mon histoire brésilienne parce que j'adore cet exemple », commence ce vétéran de l'industrie, avant d'expliquer que Huawei, ayant remporté un gros contrat pour construire le réseau de l'opérateur local Oi, n'arrivait pas à obtenir les visas pour ses centaines d'ingénieurs. « Alors ils ont affrété un navire de croisière et ils ont vécu sur ce navire, ancré en face de la côte de Rio, et ils faisaient faire des allers-retours en ferry à ses employés, assure Travis Russell. Comment une entreprise rentable peut-elle dégager le moindre profit si elle doit

envoyer des milliers d'ingénieurs, les loger, les entretenir sur tous ses sites clients, et dans le même temps affréter un navire de croisière pour les héberger ? », demande le dirigeant à son audience, par-dessus ses petites lunettes. Son incrédulité le pousse à une conclusion logique. Huawei bénéficie d'avantages impossibles à reproduire. Travis Russell, pour enfoncer ce clou, rappelle un autre épisode : « Lorsque Carlos Slim a voulu construire un réseau 4G au Mexique, la Bank of China lui a donné un milliard de dollars, avec un taux d'intérêt de 1 % s'il en dépensait 80 % chez Huawei. C'est vraiment dur pour n'importe quel fournisseur d'être en concurrence avec ce genre de contrats quand ils sont mis sur la table. »

Le problème a été identifié de longue date. Dès 2011, le P.-D.G. de l'Export-Import Bank – l'agence de crédit à l'export des États-Unis – s'en émeut dans un discours très pessimiste. « Ce que vous ne voyez pas quand vous regardez un routeur Huawei et l'une des raisons centrales pour lesquelles la croissance de l'entreprise a été si énorme, c'est qu'elle est soutenue par une ligne de crédit de 30 milliards de dollars de la Chinese Development Bank. Ce soutien permet à Huawei de réduire significativement le coût de son capital et d'offrir des financements à ses acheteurs à des taux et des conditions meilleurs que ses concurrents. Ce modèle de financement n'affecte pas que les résultats des entreprises qui tentent de les concurrencer, cela affecte aussi les résultats de notre économie, lâche Fred Hochberg. Aucun des pays du G7 ne peut fournir des niveaux de financement même voisins de ceux de la Chinese Development Bank. Cela m'empêche de dormir[31]. »

Face à ces accusations, Huawei – encore une fois – minimise. Ren Zhengfei admet certes que ses tarifs ont été excessivement agressifs par le passé. « Certaines entreprises occidentales ont fait faillite à cause de nos prix compétitifs. Je regrette ce résultat. Maintenant,

nous fixons des prix relativement élevés, plus élevés que ceux d'Ericsson et de Nokia », déclare le patron en 2019. Mais jamais Huawei ne reconnaîtra le rôle joué par les grandes banques d'État dans sa stratégie. Au contraire, le groupe ne cessera de mettre en avant deux objections. Premièrement, les lignes de crédit en question ne viennent pas financer le groupe, mais seulement ses clients qui en formuleraient le besoin. Et s'il est vrai que la Chinese Development Bank (CDP) a ouvert les vannes à hauteur de 10 milliards de dollars en 2004, puis de 30 milliards en 2009, l'utilisation réelle de ces fonds a été bien moindre. Dans une lettre ouverte[32], Ken Hu assure en 2011 que seuls 10 milliards de dollars ont été effectivement mis à disposition de ses clients par la CDP et ajoute qu'« il est important de noter que ce type de prêts ne représente qu'environ 10 % des revenus annuels de Huawei en 2010 ». Autrement dit, le succès de Huawei ne peut certainement pas être attribué à ce soutien financier.

Le jour de Noël 2019, le *Washington Post* offre un cadeau empoisonné au géant de Shenzhen, en assénant un grand coup de plus dans ce vieux dossier[33]. Le quotidien américain a fouillé méthodiquement la documentation officielle chinoise. Et au-delà des lignes de crédit des banques d'État pour 30 milliards de dollars – parmi les plus importantes de l'Histoire selon le journal –, Huawei aurait également bénéficié depuis sa création de 15 milliards de prêts d'État et autres aides, notamment sous forme de tarifs fonciers avantageux, ainsi que de 25 milliards sous forme de crédits d'impôt accordés par le gouvernement pour encourager le secteur technologique. Cette pratique de soutien à son industrie nationale n'est pas unique – le crédit d'impôt recherche en France (plus de 6 milliards d'euros en 2019[34]) ou les gigantesques rabais fiscaux accordés par Donald Trump aux multinationales américaines pour rapatrier leur cash sur le territoire américain en 2017 en sont deux

exemples. Cette dernière mesure a permis à Apple de faire une économie d'impôt de 43 milliards de dollars selon l'Institute on Taxation and Economic Policy[35] ! En ce qui concerne le soutien à Huawei, un champion national, il n'est donc pas incompréhensible. Le *Washington Post* pointe simplement son ampleur : près de 75 milliards de dollars sur trente ans.

Pour Robert Strayer, c'est un élément déterminant. Le responsable de la cybersécurité au Département d'État fait le tour de la planète pour rencontrer les dirigeants, les agences de sécurité et la presse depuis 2018 afin de les mettre en garde contre l'utilisation des équipements chinois dans les futurs réseaux 5G. Fin janvier 2020, il est à Paris. Quelques journalistes ont été invités à l'ambassade américaine, l'imposant bâtiment qui fait pendant au Crillon, sur la place de la Concorde. Passé le double contrôle de sécurité chargé de vérifier que la consigne de ne pas introduire d'ordinateur portable dans les locaux est bien respectée, le visiteur est escorté dans les grands halls néoclassiques où les portraits à l'huile des ambassadeurs ajoutent une touche de grandiose qui tranche avec le vieil ascenseur métallique, tout droit sorti d'un film d'époque sur la Seconde Guerre mondiale. Robert Strayer est dans la bibliothèque, prêt à aligner ses arguments. Dont l'un est très clair : « Huawei a reçu tellement de milliards de dollars d'aides que si l'État et les banques d'État retiraient ce financement, ils pourraient facilement exercer une pression énorme sur Huawei. […] Même en Europe, les banques chinoises représentent 20 % du financement de Huawei. Et les banques chinoises sont détenues par l'État dans la plupart des cas[36]. »

Que l'on porte un jugement positif ou négatif, Huawei est une entreprise très particulière. Mais dans les télécoms, cette étrangeté réveille vite les fantasmes. Pour la simple et bonne raison que les réseaux n'ont pas attendu la 5G pour être des nids d'espions. L'histoire

veut même que les premiers individus à hacker un réseau de télécommunications n'aient pas été chinois, ni mêmes américains, puisqu'il s'agissait de sujets bordelais de Sa Majesté Louis-Philippe Ier, répondant aux noms de François et Louis Blanc[37]. Dès 1834, ces deux filous avaient imaginé un astucieux système pour connaître les résultats de la Bourse de Paris avant tout le monde, en profitant du télégraphe de Chappe – le même dont les grands bras articulés surplombent aujourd'hui l'hôtel particulier du VIIe arrondissement où travaillent les chercheurs du centre de recherche en mathématiques de Huawei. L'arnaque fut découverte deux ans plus tard. Mais avec la montée en puissance de la capacité des réseaux, la liste des individus malintentionnés tentant d'exploiter leurs failles n'allait faire que croître.

CHAPITRE IV

Des réseaux et des espions

Pourquoi les réseaux télécoms sont-ils aussi stratégiques ? Tout simplement parce qu'en les contrôlant, il est possible de faire le plein d'informations, mais aussi de causer des dommages considérables chez un adversaire. De ce point de vue, les États-Unis n'ont sans doute rien à envier à la Chine. Les espions de Washington sont redoutables – leurs rares ratés le prouvent.

Un curieux suicide

Un cri résonne dans le corridor d'un immeuble du centre d'Athènes, non loin du parc de l'Académie de Platon. « Décrochez-le, décrochez-le ! », hurle une femme. Le corps de son fils, Kostas Tsalikidis – un ingénieur de trente-sept ans responsable de la planification réseau pour Vodafone, le premier opérateur mobile de Grèce et filiale du géant britannique des télécoms –, est suspendu à une corde, attachée aux tuyaux de la salle de bains de son appartement. La macabre découverte, en ce lundi matin du début du mois de mars 2005, a toutes les apparences d'un suicide – si ce n'est

que le jeune homme, sur le point de se marier, n'avait rien d'un dépressif. Et qu'au cours des semaines, puis des mois qui vont suivre, il apparaîtra de plus en plus clairement que sa mort est, selon toute vraisemblance, liée à une sombre histoire de piratage des réseaux téléphoniques grecs qui se soldera près de dix ans plus tard par l'émission par la justice grecque d'un mandat d'arrêt international sans précédent. Il vise en effet, comme le détaille une longue enquête au parfum de thriller du site d'information *The Intercept* parue en septembre 2015[1], un Américain d'origine grecque du nom de William George Basil. Né en 1950, l'homme a la particularité d'être un ex-diplomate de l'ambassade américaine à Athènes, et surtout un agent de la très secrète CIA.

Le 10 mars 2005, le lendemain de la mort de l'ingénieur, le Premier ministre grec Kostas Karamanlis est averti que son téléphone personnel a été espionné, ainsi que celui de sa femme, du maire d'Athènes et d'une centaine de personnalités de premier plan du pays. C'est la conclusion à laquelle viennent d'aboutir les experts techniques de Vodafone. Fin janvier de la même année, un bug leur avait mis la puce à l'oreille, quand des centaines de clients s'étaient plaints de ne pas recevoir leurs SMS. Pour comprendre les raisons de cette panne, l'opérateur avait alors contacté Ericsson, le fournisseur des équipements dont la mise à jour logicielle avait provoqué l'incident. Quelques semaines plus tard, le groupe suédois était revenu, très ennuyé, vers son client. Il avait découvert dans ses machines 6 500 lignes de code qui n'auraient pas dû s'y trouver. Le programme était écrit dans un langage informatique spécifique à l'industrie, comme le détailleront en 2007 deux universitaires dans la revue technique *IEEE Spectrum*[2], éditée par l'association professionnelle des ingénieurs électriciens et électroniciens. Grâce à ce morceau de logiciel, les appels passés vers certains numéros – dont

ceux du gouvernement – étaient automatiquement dupliqués et envoyés vers quatorze autres téléphones prépayés, permettant ainsi d'écouter et d'enregistrer toutes les conversations de l'élite grecque. Le système détournait une fonctionnalité normale des commutateurs AXE d'Ericsson installés chez Vodafone comme chez de nombreux opérateurs et qui permet aux autorités, sur mandat d'un juge, de procéder à des écoutes légales. Mais il le faisait sans que la manœuvre n'apparaisse dans aucun des systèmes de contrôle censés garder la trace de toute écoute, et donc sans qu'aucune alarme ne résonne.

Trois jours après avoir reçu le rapport alarmiste d'Ericsson – et avant même de prévenir le Premier ministre Karamanlis –, le directeur général de Vodafone Grèce avait pris une curieuse décision. Le 8 mars 2005, la veille de l'étrange suicide de son responsable de la planification réseau, il avait fait retirer le logiciel espion des quatre systèmes de commutation incriminés. Ce faisant, non seulement il faisait disparaître de précieux éléments de preuve, mais il empêchait aussi les enquêteurs d'observer le système en action pour remonter jusqu'aux espions, qui avaient immédiatement désactivé les quatorze téléphones fantômes. Était-ce volontaire ? Impossible à savoir. Pour cette malheureuse décision, qui alimentera bien des fantasmes en Grèce, Vodafone écopera tout de même de 76 millions d'euros d'amende en décembre 2006.

Malgré ce faux départ, l'enquête progresse peu à peu et les indices réunis pointent vers un suspect, que les officiels ont bien du mal à nommer. Lors d'une conférence de presse, organisée début 2006 après que le scandale de ce Watergate grec a été révélé au grand public, un ministre explique que les quatorze téléphones fantômes utilisaient tous les mêmes antennes mobiles, dans un rayon de 2 km.

Les observateurs attentifs notent rapidement que le bâtiment de l'ambassade américaine se trouve en plein milieu…

Grâce aux documents publiés en 2013 par l'ancien contractuel de la NSA, Edward Snowden, et qui vont faire vaciller le renseignement américain, l'enquête de *The Intercept* permettra d'être beaucoup plus affirmatif sur l'implication des services secrets américains dans cette affaire de piratage hors norme – au moins par sa publicité. La NSA se serait dans un premier temps branchée sur les équipements de Vodafone, avec l'assentiment des autorités grecques, pour prévenir tout risque terroriste en amont des Jeux olympiques d'Athènes de l'été 2004 – jurant de tout éteindre à l'issue de la compétition. Mais la tentation de rallumer les micros dans le dos d'Athènes a été plus forte. Malgré ces révélations, bien des questions restent ouvertes. Quelles informations ont recueilli les espions avant qu'une panne de SMS ne dévoile le pot aux roses ? Quel rôle exact a joué Kostas Tsalikidis, dont l'autopsie a été qualifiée de « grotesque » par un légiste mandaté par la famille ? William Basil, le mystérieux ex-premier secrétaire aux Affaires régionales de l'ambassade dont la justice grecque a demandé l'arrestation, a sans doute certaines des réponses. Mais il est improbable qu'il soit extradé par les États-Unis. Ou qu'il habite un jour la villa qu'il faisait construire pour ses vieux jours sur l'île de Karpathos.

La mort suspecte d'un ingénieur n'est pas un cas unique. En 2012, une autre affaire de pendaison défraye la chronique à Singapour. Shane Todd, un jeune ingénieur américain, travaille alors pour l'Institut de microélectronique (IME) de la cité État sur un programme de recherche autour du nitrure de gallium – un matériau aux propriétés fascinantes pour l'industrie des puces électroniques, aussi bien pour les téléphones portables que pour les satellites et radars militaires. Quand on le retrouvera, lui aussi, au bout d'une

corde dans sa salle de bains, sa famille dénoncera aussitôt un meurtre lié, selon elle, à de prétendues réticences du chercheur à partager ses résultats avec Huawei. Cette grave accusation, relayée par une enquête du *Financial Times*[3] quelques mois après le drame, sera pourtant démentie formellement par les autorités de Singapour, après une enquête officielle poussée. Pour le médecin légiste de Singapour, la mort de Shane Todd était, sans nul doute possible, un simple et malheureux suicide. Et peu importe qu'un confrère, mandaté par la famille, prétende le contraire. L'ingénieur souffrait de dépression et avait consulté des sites web sur le sujet. Selon les déclarations de ses anciens collègues, Shane Todd ne menait aucune recherche de nature militaire ou classifiée. Et s'il avait bien participé à deux réunions exploratoires avec Huawei, un mois avant sa mort, le projet de collaboration avec l'IME n'avait pas abouti[4]. Même l'ambassade américaine sur place reconnaîtra que l'enquête des autorités singapouriennes était « complète, juste et transparente ». En dépit de ces assurances, et d'une accusation de « recyclage de mensonges » par le ministre des Affaires étrangères de Singapour, le *Financial Times* persistera pourtant : le quotidien « maintient ce qu'il a écrit sur l'affaire Shane Todd », conclut l'article sur les résultats de l'enquête officielle[5]. Le Haut-Commissaire de Singapour au Royaume-Uni qualifiera cet entêtement de « déconcertant au plus haut point », dans la mesure où l'éditeur du *Financial Times* lui a par ailleurs assuré par écrit « ne pas remettre en cause le rapport du légiste[6] »…

Le suicide de Shane Todd est incroyablement moins litigieux, en tout cas, que celui de Kostas Tsalikidis. L'affaire du Watergate grec, suivie d'une salve d'enquêtes officielles – des parlementaires, de la justice, du régulateur… et même de la Cour européenne des droits de l'homme[7] –, reste exceptionnelle. Comme nulle autre, elle a jeté une lumière crue sur les pratiques d'espionnage sur les réseaux télécoms.

Et prouvé, s'il en était besoin, que les hommes de l'ombre n'ont pas attendu l'arrivée de la 5G ou de Huawei pour agir. Vodafone Grèce confiera d'ailleurs l'intégralité de son réseau 4G au constructeur chinois quelques années plus tard, sans jamais se retrouver dans la délicate situation de 2005. Elle montre aussi que les États-Unis, si prompts à dénoncer Pékin et les acteurs chinois des télécoms, sont bien placés pour en parler. L'Oncle Sam sait mieux que quiconque comment mésuser d'un réseau de télécommunications. Huit ans après le « suicide » de Kostas Tsalikidis, les milliers de pages de documentation interne des services de renseignement américains dérobées par Edward Snowden finiront d'ailleurs de dessiller les derniers sceptiques.

La paille et la poutre

« Mon nom est Ed Snowden, j'ai vingt-neuf ans, je travaille pour Booz Allen Hamilton en tant qu'analyste d'infrastructure pour la NSA, à Hawaï », commence le jeune homme, installé dans une chambre d'hôtel de Hong Kong, face à la caméra de Laura Poitras. La journaliste recevra plus tard un Oscar pour *Citizenfour*, son documentaire sur l'affaire Snowden. Ce 10 juin 2013, le monde découvre, en gros plan, l'homme qui ébranle les États-Unis et embarrasse jusqu'à son président, Barack Obama. Il a un bouc naissant, des cheveux en brosse et des yeux marron derrière de fines lunettes rectangulaires. Quelques jours plus tôt, le quotidien britannique *The Guardian* a publié le premier des documents classés top-secret que lui a fournis le consultant en fuite[8]. On y apprend que l'opérateur télécoms Verizon apporte quotidiennement à la NSA les données relatives aux appels téléphoniques de ses millions de clients.

Tout au long de l'été 2013, alors qu'Edward Snowden se cache et finit par trouver asile en Russie, les articles explosifs se succèdent dans la presse internationale. C'est d'abord le programme « Prism[9] » qui sort de l'ombre, avec ses quantités invraisemblables de données pompées directement sur les serveurs des géants de l'Internet : Microsoft, Yahoo, Apple, Facebook, Google… Puis les écoutes des câbles sous-marins de fibre optique – dont celui codétenu par Orange, partant de Marseille pour rejoindre Singapour – ou encore le piratage de nombreux bâtiments officiels de l'Union européenne[10], à Bruxelles comme aux États-Unis.

L'avalanche de révélations va se poursuivre pendant de longs mois. Après les opérations de collecte massive et indiscriminée, d'autres méthodes beaucoup plus ciblées apparaissent dans les documents classifiés. À la toute fin de l'année 2013, le magazine allemand *Der Spiegel*[11] décrit le fonctionnement d'une unité d'élite de la NSA, baptisée TAO (Tailored Access Operations), « une équipe de plombiers qui peut être appelée quand l'accès normal à une cible est bloqué ». Ces petits génies de la programmation savent s'introduire dans n'importe quel ordinateur, mais recourent aussi à des méthodes beaucoup plus triviales, comme l'interception de certains colis contenant du matériel de réseau avant qu'ils ne soient livrés à leur destinataire pour les trafiquer dans des ateliers clandestins. La technique, baptisée « interdiction » par la NSA, permet d'y loger des logiciels ou même des composants électroniques qui serviront de *backdoors* (portes dérobées) aux grandes oreilles américaines. Selon un document top-secret consulté par le *Spiegel*, ces détournements de colis comptent parmi « les opérations les plus productives » de l'agence et permettent à l'unité TAO d'accéder à des réseaux « dans le monde entier ». Quelques mois plus tard, le journaliste Glenn Greenwald – qui se trouvait avec Edward Snowden et Laura Poitras

dans la chambre d'hôtel de Hong Kong – en remet une couche. Avec son nouveau livre, *No Place to Hide*[12], il publie un document sur les fameuses « interdictions » de l'unité TAO, comprenant deux photos[13]. Sur l'une, on voit quatre personnes dans un atelier, méthodiquement appliquées à ouvrir au décapeur thermique un colis sur lequel apparaît en toutes lettres le mot « Cisco ». Le lendemain de sa parution, alors que la photo fait le tour d'Internet, le patron de l'équipementier américain se fend d'un courrier à Barack Obama, consulté par le *Financial Times*. « Il n'est simplement pas possible d'agir de la sorte, se plaint John Chambers. Nos clients nous font confiance pour livrer à leur porte des produits qui remplissent les plus hauts standards d'intégrité et de sécurité[14]. » Il a de bonnes raisons de s'inquiéter. Dans la foulée des révélations d'Edward Snowden, les ventes de Cisco ont chuté en Chine, mais aussi au Brésil, en Russie ou en Inde. Sur l'ensemble des marchés émergents, les commandes ont fondu de plus de 20 % en un trimestre. « Je n'ai jamais vu ça[15] », s'affole alors John Chambers.

Opération « Shotgiant »

Au milieu d'un tel vacarme, une énième bombe lâchée par le *New York Times* et le *Spiegel*, neuf mois après les premières révélations d'Edward Snowden, reçoit moins d'attention que les précédentes. Pourtant, les nouveaux documents classifiés ont une charge explosive incroyable. En plus d'avoir ciblé le président chinois Hu Jintao, le ministère du Commerce, des banques chinoises ou les deux plus grands réseaux mobiles du pays, ils montrent que la NSA a monté, dès 2007, avec l'implication du coordinateur du renseignement de la Maison-Blanche et du FBI, une opération baptisée « Shotgiant[16] »,

spécifiquement pour espionner le géant chinois des télécoms Huawei. L'effort, face à la menace « unique » que constitue le groupe de télécoms, finit par payer. En 2010, les équipes TAO parviennent à pénétrer le réseau du siège du groupe, à Shenzhen. Comme tout le trafic e-mail des employés transite par les serveurs centraux, les Américains sont en mesure de lire une bonne partie des échanges internes, y compris les messages de Ren Zhengfei ou de sa puissante numéro 2 d'alors, Sun Yafang.

Les espions comptent sur cette moisson pour parfaire leur analyse de l'organisation et établir si Huawei effectue du travail de renseignement pour le pouvoir chinois. « Si nous pouvons déterminer les plans et les intentions de l'entreprise, nous espérons que cela nous conduira aux plans et intentions de la République populaire de Chine[17] », peut-on lire sur une présentation PowerPoint de la NSA, datée de 2010. Mais les hackers américains ne comptent pas s'arrêter là. Les documents montrent que leur deuxième objectif est de se ménager des *backdoors* dans les équipements du Chinois. « Nombre de nos cibles communiquent sur des produits fabriqués par Huawei », lit-on dans la présentation. Les portes dérobées imaginées par les cracks de l'unité TAO visent à accéder à des « réseaux d'intérêt », et notamment aux « cibles de haute priorité » que sont l'Iran, l'Afghanistan, le Pakistan, le Kenya et Cuba. Le sujet est si sensible que le *New York Times* précisera dans son édition du 22 mars 2014 avoir caché des détails techniques de l'opération « Shotgiant » à la demande de l'administration Obama, pour des raisons de sécurité nationale. Pour Huawei, l'attaque est potentiellement ravageuse. En termes de communication, elle a tout de même deux aspects positifs. D'une part, et le groupe ne cessera de le faire valoir, si les services secrets américains avaient réellement trouvé des éléments compromettants, ils ne se seraient pas privés de les mettre sur la

place publique. D'autre part, comme le porte-parole de l'entreprise aux États-Unis le fait alors cruellement remarquer : « L'ironie est que ce qu'ils nous font est précisément ce qu'ils ont toujours accusé les Chinois de faire à travers nous[18]. » L'hôpital qui se moque de la charité en quelque sorte.

Les objectifs affichés de « Shotgiant » rappellent aussi que l'épouvantail agité par Washington – le matériel chinois sert les pirates chinois – est cousu de fil blanc. La réalité est qu'un attaquant doté des outils adéquats peut s'appuyer sur des équipements réseau de n'importe quel fabricant, peu importe sa nationalité. Les opportunités ne manquent pas, tant les millions de lignes de code informatique qui régissent leur fonctionnement recèlent inévitablement quelques erreurs. En 2018, Cisco a ainsi éliminé pas moins de sept *backdoors* découvertes dans ses produits[19]. En 2019, c'était au tour des routeurs de Nokia d'être pointés du doigt par les experts de Tenable Research[20] pour des failles logicielles permettant à des attaquants d'y accéder à l'insu du propriétaire. Dans le rapport annuel d'Ericsson[21], le constructeur suédois écrit noir sur blanc que ses produits peuvent contenir des vulnérabilités susceptibles d'être mises à profit par des acteurs malintentionnés et qu'elles peuvent être « impossibles à détecter ».

Ce n'est pas que de la théorie. Les exemples existent, même s'ils sont rarement de notoriété publique. Les opérations secrètes réussies restent secrètes ; et quand elles sont découvertes, les services de contre-espionnage n'en font pas toujours étalage – soit pour garder la primeur des informations, soit parce que la difficulté technique d'établir avec certitude les responsabilités les incite à la prudence. Cela n'a pas empêché en 2018 les services secrets britanniques d'épingler publiquement des pirates « soutenus par l'État russe[22] » pour des attaques sur les réseaux télécoms du royaume, survenues un

an plus tôt grâce à des failles logicielles dans certains routeurs Cisco. « Autant que nous le sachions, ces réseaux ne contenaient pas de matériel russe », relèvera Ian Levy, le directeur technique du NCSC. Andy Purdy en a fait l'un de ses arguments phare contre la mise au ban de son employeur. Pour l'ancien conseiller cyber du président George W. Bush, devenu directeur de la sécurité de Huawei aux États-Unis, le blocage ne résoudra pas le problème plus général, qui est qu'« au moins cinq nations dans le monde ont la capacité d'implanter des fonctionnalités cachées et des programmes malveillants, dans le matériel et le logiciel[23] ».

Face aux remous des révélations sur l'opération « Shotgiant », une porte-parole de la Maison-Blanche esquissera tout de même une ligne de défense : « Nous ne donnons pas les informations que nous collectons aux entreprises américaines pour améliorer leur compétitivité à l'international ou améliorer leurs résultats. Bien des pays ne peuvent en dire autant[24]. » En d'autres termes, oui, nous espionnons, mais ce n'est pas de l'espionnage industriel… Outre que ce n'est pas démontré, font valoir les critiques, le vol de secrets industriels est-il réellement une motivation pire que le sabotage pour hacker les réseaux étrangers ? Car ce cap a déjà été franchi. Et, de l'avis de bien des spécialistes, ce sont les États-Unis qui ont ouvert la boîte de Pandore en concevant, avec les Israéliens, le programme « Stuxnet ». Découvert en 2010, ce logiciel sophistiqué agissait sous les radars depuis plusieurs années dans le but de ralentir le programme d'enrichissement d'uranium de l'Iran. Pour cela, il modifiait – à l'insu des systèmes de contrôle – le comportement des valves de contrôle des gaz produites par l'Allemand Siemens, faussant le fonctionnement des centrifugeuses de la centrale de Natanz. Pour masquer leurs traces, les concepteurs avaient mis en place de faux sites web de fans de football, sortes de paravent au-dessus des

serveurs de contrôle de « Stuxnet » afin que la remontée de rapports apparaisse comme de banales connexions d'un employé consultant les résultats de son équipe favorite. Dix ans avant la 5G et ses promesses de révolution industrielle, le monde découvre la première « cyberbombe ». Invisible, intraçable, capable de gripper des usines stratégiques, elle fera des petits. Deux ans plus tard, alors que commence le mois sacré de Ramadan, un autre missile virtuel, baptisé « Shamoon », atteint l'Arabie saoudite et paralyse le premier groupe pétrolier mondial, Saudi Aramco. Est-ce une réponse des Iraniens à « Stuxnet » ? Les experts le pensent. Au-delà des éléments techniques, ils ont retrouvé, caché dans le code informatique de « Shamoon », une image montrant un drapeau américain en flammes, comme une revendication. Une nouvelle forme de guerre est née. La Chine, comme d'autres, peut légitimement se retourner vers Washington et demander : qui a lancé les hostilités ?

Les hackers de Shanghai

Ils ont pour petits noms « UglyGorilla » ou « Superhard ». Cela pourrait prêter à sourire si leurs méfaits supposés n'étaient pas si graves. Dans un document de 76 pages, accompagné de volumineuses annexes techniques, la société de cybersécurité Mandiant (fondée par un ancien officier de l'US Air Force et rachetée par la suite par son concurrent FireEye) détaille en 2013 les agissements de plusieurs hackers appartenant à un même groupe, connu sous les noms d'« APT1 », « Comment Crew » ou encore « Byzantine Candor »[25]. Depuis plusieurs années, ils sont à l'origine d'une série d'infiltrations complexes, dans au moins 141 entreprises, majoritairement américaines, avec la particularité de rester en

planque dans les réseaux des victimes pendant un an en moyenne (dans un cas, près de cinq ans) et de siphonner à chaque fois des téraoctets de données. Les experts de Mandiant se sont acharnés à suivre les maigres indices laissés ici et là par les voleurs, remontant la piste des adresses IP utilisées jusqu'à un quartier de Shanghai où, six ans plus tôt, a été construit un grand immeuble blanc de douze étages, protégé par des grilles noires et une poignée de militaires en uniforme. C'est le siège de l'unité 61398 – le nom de code militaire du 2e bureau du 3e département de l'État-major de l'Armée populaire de libération –, chargé des opérations cyber. Pour Mandiant, l'affaire ne fait pas de doute. APT1 n'est autre que l'unité 61398. Le rapport se permet même un quasi-sarcasme, évoquant la seule autre possibilité : celle qu'une organisation secrète et bien dotée, remplie de locuteurs chinois, avec un accès direct à une infrastructure de télécommunications basée à Shanghai, soit engagée dans une énorme campagne d'espionnage industriel sur plusieurs années, juste à côté des bureaux de l'unité 61398 et avec des activités correspondant aux missions connues de l'unité 61398… La Chine démentira à toute force un rapport « non professionnel ». Mais moins d'un an plus tard, un poster fait le tour du monde. Sous un bandeau rouge marqué « Wanted by the FBI[26] », comme dans un vieux western, s'affichent les photos de cinq hommes – tous officiers de l'unité 61398 et accusés de piratage informatique et d'espionnage économique. C'est la première fois que des acteurs étatiques sont inculpés pour des actes de hacking. Et ce n'est pas la dernière fois que des agents chinois défraient la chronique.

Xu Yanjun, par exemple, n'est pas un simple espion. C'est un officier de renseignement chinois, le directeur adjoint pour la région de Shanghai d'une agence du ministère de la Sécurité d'État (le ministère chargé du renseignement et du contre-espionnage).

Pourtant, s'il se trouve dans le centre historique de Bruxelles, en ce dimanche de Pâques 2018, c'est pour une mission « à l'ancienne ». Il doit rencontrer un ingénieur américain de la branche Aviation de General Electrics, en provenance de Cincinnati, à 7 000 km de là, qui a promis de lui livrer des documents confidentiels. Le temps est frais et le ciel dégagé. Les cloches de l'église Saint-Nicolas, à côté de la grand-place, font écho à celles de Sainte-Catherine, 500 m plus bas. Mais Xu Yanjun n'a pas le loisir d'en profiter. Démasqué par le FBI, son contact chez GE Aviation n'est jamais arrivé au rendez-vous. À la place, c'est la police belge qui attendait le maître espion pour lui passer les menottes. Six mois plus tard, Xu Yanjun monte dans un avion, en direction des États-Unis. Inculpé de tentatives d'espionnage économique et de vols de secrets commerciaux, il encourt 25 ans de réclusion. « Cette extradition sans précédent d'un officier de renseignement chinois met en lumière la supervision directe par le gouvernement chinois de l'espionnage économique à l'encontre des États-Unis[27] », se félicite alors le FBI.

Un profil tel que celui de Xu Yanjun ne s'est jamais retrouvé devant un tribunal américain. Mais l'occasion est trop belle pour les États-Unis de dénoncer ce que ses autorités, unanimes, considèrent comme une exception chinoise. Selon le Département de la justice américain[28], environ 80 % des affaires d'espionnage économique qui lui sont remontées ont pour bénéficiaire supposé l'État chinois. Dans bien des cas, il s'agit, comme pour l'ingénieur de GE Aviation, de cadres d'entreprises américaines approchés pour des conférences scientifiques ou de pseudo-partenariats universitaires. Excédé, le FBI a même produit en 2015 un film de fiction d'une quarantaine de minutes, *The Company Man*[29], inspiré de faits réels et dans lequel deux Chinois tentent de dérober une technologie d'isolation thermique à une entreprise américaine, qu'il a fait visionner à plus de

1 300 cadres à travers le pays pour les mettre en garde. Mais la vaste majorité des secrets industriels s'envole probablement pour Pékin sans qu'aucun contact humain ne soit nécessaire. C'est en tout cas ce que craignent les spécialistes de cybersécurité qui, rapport après rapport, dénoncent l'ampleur des piratages attribués avec une forte probabilité aux hackers chinois.

« Cloud Hopper », un coup de génie

Alors que les exemples se succèdent d'entreprises et d'administration pillées, Barack Obama tape du poing sur la table. En septembre 2015, une semaine avant la première visite officielle du président Xi Jinping à Washington, il annonce publiquement se tenir prêt à mener des « actions compensatrices[30] » vis-à-vis de Pékin. Le président dit comprendre et accepter que la Chine pratique l'espionnage et essaie d'obtenir des secrets d'État – exactement comme les États-Unis – mais juge le vol de secrets industriels fondamentalement différent. « Nous le considérons comme un acte d'agression qui doit prendre fin », menace le locataire de la Maison-Blanche. Quelques jours plus tard, en compagnie de Xi Jinping, il annonce être parvenu à une « position commune » sur une absence totale de soutien étatique à des opérations de cyber-espionnage commercial.

Si trêve il y eut jamais, elle fut de courte durée. Dès 2016, le vol massif de données par les cyber-espions chinois bat son plein, alors même que l'attention du public s'est reportée sur les ingérences russes dans l'élection présidentielle américaine. C'est en tout cas ce qui ressort de plusieurs affaires qui ont émergé ces dernières années, dont la plus emblématique est sans doute l'opération « Cloud

Hopper », rendue publique par l'inculpation en décembre 2018 de deux hackers chinois liés au ministère de la Sécurité d'État[31]. Pendant des années, ces membres d'un groupe baptisé « APT10 » ont réussi un coup de génie, en piratant une dizaine des plus importants sous-traitants informatiques de la planète. Or ces entreprises, dont les plus connues ont été identifiées dans une enquête de Reuters[32] comme IBM, Hewlett Packard Enterprise, Fujitsu ou Tata Consultancy Services, fournissent leurs services de cloud – c'est-à-dire de stockage informatique et de calcul à distance – à une foultitude de clients. Autant d'autres entreprises qui se sont ainsi trouvées à portée des hackers, parmi lesquelles le géant minier brésilien Vale, le constructeur des sous-marins nucléaires américain Huntington Ingalls, le spécialiste suisse d'agrochimie Syngenta (qui sera racheté par un groupe chinois pour 43 milliards de dollars en pleine opération « Cloud Hopper ») ou l'équipementier télécoms suédois Ericsson.

Trop, c'est trop. Face à ce qu'un ancien patron de la NSA, le général Keith Alexander, dénonçait dès 2012 comme « le plus grand transfert de richesse de l'Histoire[33] », le président Donald Trump est déterminé à agir, à sa façon. Le pillage informatique rejoint la longue liste des infractions commerciales dont il accuse la Chine, à côté des subventions indues à ses entreprises, des transferts forcés de technologie ou des entraves à la libre concurrence sur son territoire. Après avoir confié une enquête à son représentant au Commerce, Robert Lighthizer, sur les violations de propriété intellectuelle dont se rendrait coupable la Chine, il relève les droits de douane sur certaines importations chinoises, pour un montant total de 50 milliards de dollars, à l'été 2018. Un bras de fer commercial comme jamais le monde n'en a connu s'engage. Il ne fera que se durcir dans les deux années suivantes, sans que l'Amérique ne constate d'amélioration sur

le plan des vols de données. « Le FBI ouvre un nouveau dossier de contre-espionnage en lien avec la Chine environ toutes les dix heures, assurait son directeur, Christopher Ray, début juillet 2020. En ce moment même, la Chine travaille à compromettre des organisations de santé américaines, des entreprises pharmaceutiques et des institutions académiques menant des recherches essentielles sur le Covid-19[34]. »

Robert Strayer, le fonctionnaire du Département d'État chargé de savonner la planche à Huawei, ne pouvait pas manquer d'intégrer cet élément à son argumentaire. « Les Chinois sont derrière le plus vaste vol de propriété intellectuelle de l'histoire moderne avec l'attaque Cloud Hopper, explique-t-il début 2020 dans la bibliothèque de l'ambassade américaine à Paris. C'est ce qu'ils pourraient faire s'ils contrôlaient les réseaux 5G[35]. » Avec sa raie sage sur le côté et ses dents blanches qui saillent à chaque sourire, le responsable de la cybersécurité donne l'impression de tourner dans une réclame vantant une excellente lessive ou un dentifrice révolutionnaire. Le rabâchage de son mantra anti-Huawei est aussi entêtant qu'un slogan de campagne publicitaire. Cette détermination est en réalité à la hauteur de la menace que représente la 5G dans l'esprit de l'administration américaine.

Les murs ont des oreilles

Dans cet océan d'opérations d'espionnage croisées, la responsabilité du premier fournisseur mondial de réseaux mobiles est pourtant rarement mise en cause. L'affaire la plus retentissante avec laquelle Huawei a dû se démener ces dernières années est celle du piratage du siège de l'Union africaine (UA) à Addis-Abeba, révélée

par le journal *Le Monde*[36] début 2018, et confirmée par le *Financial Times*[37] quelques jours plus tard. Six ans plus tôt, le président chinois Hu Jintao est dans la capitale éthiopienne pour l'inauguration du tout nouveau siège de l'Union africaine. Au cœur de la ville, les bâtiments de l'organisation de coopération panafricaine dominent le paysage. À côté d'une grande structure sphérique qui accueille la salle de conférences de 2 500 places où se réunissent les chefs d'État de tout le continent lors de la conférence bisannuelle de l'Union, un gratte-ciel de 117 m de haut héberge les bureaux et salles de réunion. Si Hu Jintao est présent ce jour-là, c'est pour la simple et bonne raison que cet immeuble est un cadeau de la Chine au continent, livré clé en main après trois ans de travaux et un investissement estimé à 200 millions de dollars. Mais une mauvaise surprise attend les bénéficiaires de tant de générosité. En janvier 2017, selon l'enquête du *Monde*, les informaticiens de l'UA notent une bizarrerie. Les serveurs de l'organisation semblent curieusement occupés pendant deux heures, en plein milieu de la nuit, alors même que plus personne ou presque ne travaille. En essayant de comprendre l'anomalie, les équipes techniques découvrent alors que les données de l'organisation sont massivement extraites nuitamment pour être envoyées sur des serveurs à plusieurs milliers de kilomètres, quelque part à Shanghai. Pire, ces vols se seraient étalés sur les cinq années qui séparent l'inauguration du bâtiment et la découverte de ce que *Le Monde* décrit comme des « portes numériques dérobées (*backdoors*) qui donnent un accès discret à l'intégralité des échanges et des productions internes de l'organisation ».

Les observateurs sont alors nombreux à pointer du doigt l'entreprise qui, sur son propre site, se vante d'avoir mis en place le système d'information rutilant du bâtiment. Huawei, puisqu'il s'agit d'elle, se défend à toute force et déclare que les allégations sont

« complètement sans fondement » : « Notre participation dans les infrastructures de centre de données pour le siège de l'Union africaine en Éthiopie comprend deux solutions, dont aucune n'a accès à des données client ou business, écrit le groupe de Shenzhen dans un communiqué. Les solutions fournies à l'UA étaient contrôlées, supervisées et opérées par les équipes informatiques de l'organisation et Huawei n'avait aucun accès aux données de l'UA[38]. » Ren Zhengfei, interrogé sur le sujet début 2019, répondra lui aussi que « pour la violation des équipements utilisés par l'Union africaine, cela ne concernait pas Huawei[39] ». Et plus largement, sur le sujet des *backdoors*, le patron est catégorique. Huawei n'y a jamais eu recours, et n'y recourra jamais, pour la simple raison que ce serait suicidaire. Que se passerait-il si un de ses clients découvrait le pot aux roses ? L'activité s'effondrerait. L'entreprise, avec ses centaines de milliers de salariés, serait désemparée. « Nous préférerions fermer l'entreprise plutôt que de faire quoi que ce soit qui nuise à l'intérêt de nos clients[40] », martèle Ren Zhengfei face à la presse.

À la suite des enquêtes du *Monde* et du *Financial Times*, l'Union africaine dément aussi catégoriquement tout vol de données, par la voix du président de la commission, Moussa Faki. Le Premier ministre éthiopien et des officiels chinois nient également l'existence d'un piratage. « C'est très embarrassant. Ils ont dû tout démonter », commentera pourtant en privé un dirigeant du secteur un an plus tard, lors du Mobile World Congress de Barcelone. Piratage chinois ou pas, la meilleure façon pour Huawei de montrer que le groupe n'avait rien à se reprocher était de resserrer ses liens avec l'UA. À l'été 2019, le vice-président du groupe pour l'Afrique, Philippe Wang, est donc à Addis-Abeba et pose, pour la photo, avec un diplomate ghanéen. Thomas Kwesi Quartey, vice-président de la commission de l'UA, porte une chemise ouverte à motifs africains

noire et blanche ; le businessman chinois, un costume strict égayé par une cravate rose. Les deux hommes tiennent à la main un protocole d'accord tout juste signé. Huawei étend son partenariat avec l'UA dans plusieurs domaines : le haut débit, l'Internet des objets, le cloud, l'intelligence artificielle et la 5G. Voilà de quoi faire taire les mauvaises langues. Jusqu'à la prochaine fois.

Les geôles de Varsovie

C'est une scène digne d'un roman d'espionnage de la guerre froide. Le matin du 8 janvier 2019, à Varsovie, en Pologne, la police fait une descente et arrête un ancien diplomate féru de technologies, soupçonné d'être un agent à la solde de l'étranger. Mais le Mur est tombé depuis belle lurette. L'appartement que la sécurité intérieure polonaise vient d'investir est celui d'un homme d'affaires chinois. Les fonctionnaires saisissent quelques photos et tout le matériel électronique avant de repartir avec le suspect, Wang Weijing, trente-sept ans. Ex-attaché culturel du consulat de Gdansk, il travaille depuis 2011 pour la filiale polonaise de Huawei, où il a été pendant cinq ans le responsable des affaires publiques avant de prendre un poste de responsable des ventes. Ce même jour où l'appartement de Wang Weijing se retrouve sens dessus dessous, un autre raid des autorités vise le siège d'Orange Polska, le plus grand opérateur du pays et filiale du groupe français de télécommunications. Les policiers veulent en savoir plus sur les agissements d'un salarié, Piotr Durbajlo. Ancien des services secrets polonais, ce spécialiste de cybersécurité a fait partie des équipes du régulateur polonais des télécoms avant de se mettre au service de l'opérateur, comme consultant. Selon une enquête de l'agence Reuters[41], Piotr Durbajlo aurait travaillé pour

l'Agence de sécurité intérieure du pays pendant plus de six ans, dont trois années au sein de l'université militaire de technologie de Varsovie sur un sujet très délicat : la création d'un système de supervision pour mettre à l'abri des oreilles indiscrètes les informations sensibles transitant sur des réseaux de fibre optique. Accusé d'espionnage, il encourt dix années de réclusion. Tout comme son ami Wang Weijing.

Les deux hommes se connaissent bien. Leur relation remonte au moins à 2013, l'année où Piotr Durbajlo franchit pour la première fois les portes du siège de Huawei, à Shenzhen, avec une délégation du régulateur polonais. Ils se rendront ensemble en Chine à deux autres reprises. Une fois dans le cadre du travail dans les locaux de Huawei, et une fois pour un voyage touristique avec toute la famille du Polonais, pour qui Wang Weijing fait le guide. Le cadre de Huawei décrit Piotr Durbajlo comme « sans doute [s]on meilleur ami polonais[42] », dans une lettre d'avril 2019 transmise par son avocat et écrite depuis la prison de Warsaw-Bialoleka, où il est incarcéré. Entré en service en 1961, ce vaste centre de détention aux murs de béton surmontés de rouleaux de barbelé est tristement célèbre pour avoir accueilli, dans ses petites cellules grises et surpeuplées, des membres du syndicat Solidarnosc poursuivis par le régime communiste. Ironie du sort, c'est aujourd'hui un supposé espion du PCC qui y est derrière les barreaux. Son complice présumé a, lui, été libéré sous caution après six mois sous les verrous.

Pour le groupe de Shenzhen, qui compte 900 salariés en Pologne, l'affaire est problématique. Comme ailleurs dans l'est de l'Europe, Huawei est très bien installé dans le pays. En dehors d'Orange Polska, le groupe fournit aussi la majeure partie du réseau de Play – devenu en 2020 une filiale du groupe Iliad de Xavier Niel – et de T-Mobile, la filiale locale de l'Allemand Deutsche Telekom. Avec l'arrivée de la 5G,

Varsovie réfléchit comme toutes les capitales européennes à durcir les conditions d'accès aux équipementiers chinois. Ici aussi, Robert Strayer, l'envoyé du Département d'État américain, est venu faire son speech anti-Huawei. Depuis sa cellule, Wang Weijing pointe que « trouver un soi-disant espion chez Huawei est une excuse parfaite pour dégager Huawei de la Pologne et d'ailleurs ». Il est sans doute au courant que, dans la foulée du scandale, le patron de la cybersécurité polonaise, Karol Okonski, a déclaré sur la première chaîne de radio polonaise, RMF, que le pays réfléchissait à mettre en garde ses opérateurs à l'égard du géant chinois, voire à lui fermer l'accès aux marchés télécoms du pays. Pour ne rien arranger pour le groupe chinois, la Pologne a d'autres éléments à prendre en considération. Varsovie ne veut pas contrarier Washington, dans l'espoir que quelques milliers de soldats américains quitteront leurs bases allemandes pour venir s'établir sur le sol polonais. Ce projet, qui porte le surnom de « Fort Trump », est jugé stratégique face à la menace du grand voisin russe. Que pèsera Huawei dans cette équation ?

Pour contenir l'incendie, le groupe réagit énergiquement. Dans la foulée de l'arrestation, Wang Weijing est licencié pour avoir « porté atteinte à la réputation » de l'entreprise. Huawei affirme n'avoir rien à voir avec les agissements supposés de son salarié. Le porte-parole des services polonais, Stanislaw Zaryn, apporte sa pierre à la défense chinoise, en déclarant : « Il y a un climat mondial qui tend à parler surtout de cette entreprise. Pour nous, cette enquête particulière concerne deux individus. Les menaces dans l'industrie de télécommunications sont un problème séparé. » Mais dans le tweet[43] annonçant l'arrestation des deux supposés espions, le même Stanislaw Zaryn met en copie les comptes Twitter du Département d'État américain, de la CIA et du FBI. D'ailleurs, s'il fallait une preuve

que l'Amérique analyse l'affaire sous ce prisme, les déclarations du vice-président américain lors de sa visite en Pologne le mois suivant l'événement lèvent tout doute. L'arrestation d'« un cadre de Huawei et d'un citoyen Polonais accusé d'avoir coopéré avec lui, assure Mike Pence, démontre l'engagement de votre gouvernement à s'assurer que notre secteur des télécommunications n'est pas compromis d'une manière qui menace notre sécurité nationale[44] ».

Cet accrochage est révélateur, car chaque partie le voit sous son propre jour. Pour Huawei, c'est une mauvaise publicité très dommageable et, surtout, une criante injustice puisqu'aucun manquement de sa part n'a été démontré. Pour ses détracteurs, c'est une preuve de plus qu'il y a décidément quelque chose qui cloche avec le groupe de Shenzhen. Les États-Unis en sont persuadés, et depuis bien longtemps – à une époque où les smartphones n'existaient pas et où peu de gens connaissaient le logo aux huit pétales rouges.

CHAPITRE V

Les vieilles rancœurs de l'Oncle Sam

Huawei s'est imposé partout dans le monde, sauf aux États-Unis. Et ce n'est pas faute d'avoir essayé, mais bien avant que la 5G ne devienne un sujet de préoccupation Outre-Atlantique, le groupe de Shenzhen avait déjà éveillé plus que la méfiance à Washington. Pendant vingt ans, les accusations les plus diverses – plagiat, vol, etc. – ont plu sur l'équipementier chinois. Au point de lui faire quasiment jeter l'éponge…

La fibre de Saddam

Une série d'éclairs zèbre le ciel nocturne, tandis que retentissent les sirènes antiaériennes, poussant les habitants de Bagdad à se terrer pour échapper aux missiles. Ce vendredi 16 février 2001 [1], cela faisait presque deux ans que le funeste signal n'avait plus été entendu. Mais cette nuit-là, une vingtaine de chasseurs américains et britanniques sont passés à l'attaque. Leurs bombes téléguidées ont frappé cinq sites des alentours de la capitale, faisant deux victimes civiles [2] et de nombreux blessés. Dans les heures qui suivent, la quasi-totalité des

pays arabes – pourtant alliés de Washington depuis que la première guerre du Golfe a stoppé l'offensive de Saddam Hussein sur le Koweït dix ans plus tôt – dénonce les frappes. Fraîchement nommé secrétaire d'État, Colin Powell fait la tournée des capitales régionales pour justifier l'opération. Il s'agissait, assure-t-il, de détruire des infrastructures de défense antiaérienne. Améliorées en cachette par Saddam Hussein, elles menaçaient la sécurité des patrouilles alliées contrôlant les zones d'exclusion aérienne mises en place en 1991. Dernièrement, Washington avait acquis la certitude que, pour accélérer les liaisons entre les systèmes radar et les rampes de missiles, un réseau de fibre optique avait été construit. Des sources américaines expliquent, dans un article du *Washington Post* du 1er mars 2001[3], que l'entreprise qui a bravé les sanctions des Nations unies pour moderniser ainsi l'arsenal irakien est un groupe de télécoms chinois, encore largement inconnu du grand public, du nom de Huawei.

Avec vingt ans de recul, le débat qui s'installe alors est fascinant, tant il porte en lui les germes de bien des ennuis à venir. Mi-2001, les analystes politiques estiment que Huawei ne répond sans doute pas à des consignes officielles, mais est simplement mû par l'appât du gain. Contrairement aux grands conglomérats énergétiques publics dont les agissements en Irak, mais aussi au Soudan ou en Birmanie, font également grincer Washington – il s'agit en effet d'une entreprise privée. Dans le même temps, cette violation des sanctions internationales et des lois américaines sur le transfert de technologies vers l'Irak pousse des chercheurs d'une ONG de lutte contre la dissémination nucléaire à publier une tribune[4] appelant le président George W. Bush à en tirer toutes les conséquences en… coupant Huawei de ses indispensables fournisseurs américains, dont Qualcomm et IBM.

Face aux accusations, Huawei dément, par la voix d'une responsable marketing au Moyen-Orient qui déclare à l'agence *Associated Press* : « Notre entreprise ne mène… que des projets en Irak autorisés par les Nations unies[5]. » Malgré ces dénégations, la Chine accepte le principe d'une enquête. En coulisse, des officiels chinois auraient promis à Colin Powell de demander à leurs entreprises de télécoms de cesser tout travail sur le site. La tension semble retomber. En juin, dans le cadre d'un échange de bons procédés diplomatiques, et pour « alléger les souffrances du peuple irakien », les États-Unis lèvent partiellement l'embargo sur des dizaines de millions de dollars de ventes d'équipements télécoms à l'Irak. Le lobbying des équipementiers pour avoir accès au programme « Pétrole contre nourriture » a payé, ils vont pouvoir reprendre les affaires en Irak – dont les infrastructures ont bien besoin d'un gros lifting. Huawei, comme ses pairs, compte être de la fête. Un gros contrat, qu'il a signé en 1999, attend ce feu vert des Nations unies depuis trois ans. Mais quelques semaines plus tard, la situation se retourne. Après qu'un missile irakien s'est curieusement approché d'un avion furtif américain, les États-Unis acquièrent la conviction que Huawei poursuit ses activités de modernisation antiaérienne. Furieux, ils bombardent début août les mêmes installations déjà ciblées six mois plus tôt. Huawei a-t-il compris le message ? Toujours est-il que le 9 septembre, le ministre des Communications irakien[6] annonce que Huawei se désiste de son contrat de 1999. Le groupe chinois parlera plus tard d'une « décision business ». Dans le même temps, le français Alcatel, profitant de la levée de l'embargo américain, signe la vente de 75 millions de dollars d'équipements. Les États-Unis n'auront pas le loisir d'épiloguer. Quarante-huit heures plus tard, le monde bascule. Deux tours se sont effondrées à New York.

La folle rumeur de Kaboul

Les cendres du World Trade Center flottent encore dans les rues quand George W. Bush lance sa « guerre contre le terrorisme ». La rhétorique de l'administration américaine est binaire. « Êtes-vous dans notre équipe ou non ? Il n'y a pas de zone grise[7] », lance le vice-secrétaire d'État Richard Armitage à des officiels pakistanais. En Chine, la question ne se pose guère. En butte depuis des années aux séparatistes islamistes de la région du Xinjiang, qui s'entraînent souvent en Afghanistan avant de repasser la frontière pour poser des bombes ou assassiner des officiels chinois, le président Jiang Zemin voit tout l'intérêt de s'inscrire dans le sillage des Américains. Le seul hic est que Pékin est fortement soupçonné de continuer à entretenir des relations, notamment commerciales, avec les autorités de Kaboul[8]. Après tout, les deux pays sont voisins. Ils partagent une frontière commune, de 76 km, au fond de l'étroit corridor de Wakhan – celui que parcourut jadis Marco Polo. Mais depuis cinq ans, le pouvoir à Kaboul est exercé par les Talibans, qui hébergent Oussama Ben Laden, le cerveau des attentats et l'homme le plus recherché du monde.

Un de ces soupçons va se faire jour en Inde. Au début du mois de décembre 2001, les Talibans ont déjà été chassés de Kaboul par les GI's. Mais le spectre des islamistes s'invite dans les colonnes de deux des principaux quotidiens du pays – *The Hindustan Times* et *The Economic Times*. Les deux journaux affirment que les services secrets indiens – aiguillés par leurs homologues américains – s'inquiètent que la filiale locale d'un groupe chinois ait développé des systèmes de télécommunications pour les fondamentalistes afghans. Il s'agit de Huawei, encore une fois. Solidement implanté en Inde, le groupe a installé deux ans plus tôt un centre de développement logiciel dans le

sud du pays, plus précisément à Bangalore. La capitale de l'État du Karnataka est le cœur de la tech indienne, en plein boom en ce début de siècle grâce à ses ingénieurs bien formés, anglophones et bon marché. Les géants de la sous-traitance informatique comme Accenture ou CapGemini y délocalisent des pans entiers de leur activité, tandis que des groupes locaux tels Tata Consultancy Services, Infosys ou Wipro rêvent de leur faire de l'ombre. Cette dynamique n'a pas échappé à Huawei, qui offre des salaires très attractifs afin de s'attirer les services de 500 techniciens et ingénieurs, dont un tiers vient de Chine, pour travailler sur des logiciels – notamment dans la perspective de la 3G. Tout va donc pour le mieux jusqu'à ce lundi 10 décembre 2001. Quand les autorités régionales du Karnataka prennent connaissance des articles arguant que ces informaticiens chinois auraient pu en réalité travailler pour les Talibans, c'est l'affolement. Trois mois à peine après le 11 septembre, il ne fait pas bon être associé au début de l'ombre d'un terroriste. Les dirigeants de la filiale sont immédiatement convoqués par les autorités[9], mais ils sont en déplacement en Chine et il faudra attendre la fin de la semaine pour les entendre. Le groupe, lui, fustige sans attendre des insinuations « sans fondement » et exclut formellement avoir eu quelque relation que ce soit avec les mollahs[10]. De fait, après une rapide enquête, les autorités du Karnataka, ne trouvant absolument aucune preuve ni indice, blanchissent Huawei[11]. Mais le poison du doute a été instillé, si lent à se dissiper. Et, encore une fois, les services secrets des États-Unis pourraient bien être l'empoisonneur.

Pourtant, en cette fin d'année 2001, les nouvelles en provenance de l'autre rive du Pacifique sont loin d'être toutes mauvaises pour Huawei. En octobre, le groupe américain Emerson a racheté la filiale de Huawei qui produit des blocs d'alimentation électrique – Avansys – pour 750 millions de dollars. L'opération est un record pour une

acquisition étrangère en Chine. Elle permet au groupe de Shenzhen de se séparer d'une activité périphérique en engrangeant une coquette somme pour financer ses recherches dans la 3G. Quelques semaines plus tard, Huawei signe un important accord avec le Californien Qualcomm pour avoir accès, sous licence, à son massif portefeuille de brevets pour la 3G. Des accords similaires sont conclus avec Intel, Sun ou Philips Semiconductors (la filiale du géant néerlandais, numéro 2 des puces électroniques en Europe, sera renommée NXP en 2006 après sa scission d'avec son conglomérat d'origine). Huawei est en train de devenir un acteur qui compte à l'international. Le groupe peut commencer à rêver du Graal, c'est-à-dire la conquête du marché américain. En dépit des casseroles que les services secrets de l'Oncle Sam semblent résolus à lui attacher, Ren Zhengfei ne se décourage pas. Cette même année 2001, le groupe enregistre sa première filiale aux États-Unis. Son nom – FutureWei – sonne comme un programme. Mais en à peine deux ans, il sera rendu caduc par un procès médiatisé, intenté par un des champions de la tech américaine.

Copié-collé

Pour ses premiers bureaux américains, Huawei a choisi Plano, une paisible petite ville texane, dans la banlieue de Dallas. La métropole est un haut lieu des télécoms. À une demi-heure des locaux de FutureWei, on trouve en effet le siège d'AT&T – premier opérateur américain, héritier du groupe fondé par l'inventeur du téléphone, Graham Bell en personne. Le maire de Plano est ravi d'accueillir une nouvelle entreprise[12], en ces temps de crise économique post-éclatement de la bulle Internet où les investissements se font rares. Le

groupe chinois, lui, voit dans ces temps de disette une opportunité. Les opérateurs télécoms et les entreprises en général sont à la recherche d'économies. Le moment est idéal pour leur proposer des produits bon marché et de bonne qualité – la marque de fabrique de Huawei, qui compte bien se faire une place au soleil pour commencer sur le marché des routeurs, la chasse gardée de Cisco. Avec 3 milliards de dollars de revenus en 2001, le groupe de Shenzhen commence à attirer l'attention de l'industrie. « Ce n'est pas ce que j'appellerais une start-up émergente, explique un analyste du Crédit lyonnais au *Dallas Business Journal*. D'ici cinq à sept ans, ce sera un concurrent majeur, non seulement sur la scène mondiale mais jusque dans l'arrière-cour des fabricants nord-américains[13]. » Ce que ce spécialiste ne pouvait prévoir, pas plus que Huawei, c'est qu'un obstacle judiciaire allait se mettre en travers de la route.

À peine un an après que Huawei a commencé à écouler ses produits sur le marché américain, une plainte est déposée auprès de la cour de district fédérale pour le Texas oriental[14]. Elle émane de Cisco et son contenu est ravageur. Le groupe américain s'est procuré un routeur de la gamme Quidway de son concurrent chinois. Huawei en fait une large promotion, expliquant que ces produits ont les mêmes fonctionnalités et performances que les routeurs de Cisco. « La seule chose qui nous différencie, c'est le prix[15] », clament les publicités de Huawei dans les magazines spécialisés. Auprès de ses futurs clients, l'industriel chinois assure qu'ils n'auront aucun mal à changer de fournisseur et à prendre en main ses produits. Et pour cause : ce sont des copies presque conformes de ceux de son concurrent américain, à en croire les ingénieurs de Cisco. Sur 25 pages, la plainte décrit l'ampleur du plagiat. Non seulement les instructions du code source sont similaires, mais aussi tous les commentaires en anglais qui les accompagnent. Ces « empreintes

digitales » sont confondantes, selon Cisco. Il est improbable, pour ne pas dire impossible, que les développeurs de Huawei aient écrit des centaines de lignes de texte avec exactement les mêmes mots, dans le même ordre. Même un bug dans le logiciel de Cisco se retrouve, identique, chez Huawei. Quant au manuel utilisateur, fourni sur un CD-Rom, des portions entières apparaissent comme de vulgaires copié-collés et les légères modifications apportées ici et là pour brouiller les pistes ne sont même pas cohérentes.

Chez Huawei, c'est la panique. En pleines festivités du Nouvel An chinois, l'état-major est rappelé en urgence au siège. Ce n'est pas que l'on découvre le problème. Trois mois plus tôt, des dirigeants de Cisco ont fait le déplacement en Chine et ont été reçus, au très chic hôtel Shangri-La de Shenzhen, par Ren Zhengfei en personne[16]. Après avoir exposé leurs griefs, les Américains ont déjà exigé une reconnaissance de culpabilité, le retrait des produits incriminés du marché américain et un gros chèque de compensation. Mais Huawei s'est contenté de rappeler certains de ses routeurs. Furieux, Cisco a interprété la manœuvre comme une tentative de faire disparaître des preuves et a déposé plainte – ce que le groupe aurait sans doute préféré éviter, de peur des répercussions éventuelles en Chine, où le groupe fait de juteuses affaires. De fait, dès l'année 2004[17], le rapport annuel de Cisco fait état de « faiblesses dans [ses] ventes en Chine » et ne cessera d'y perdre des plumes face à la concurrence locale. Mais début 2003, alors que l'affaire atterrit sur le bureau d'un juge de Marshall, au Texas, c'est Huawei qui se retrouve face au mur. Échouer dans un tel procès signifierait perdre beaucoup d'argent, mais aussi l'accès au marché américain et vraisemblablement la confiance de certains grands clients internationaux. Avec un bataillon d'avocats, Huawei va donc entamer des négociations. En 2004, un accord – confidentiel – est trouvé entre les deux groupes et la plainte est

abandonnée. Le public n'en saura pas plus, si ce n'est à travers un post de blog de 2012, signé de Mark Chandler[18]. Le directeur juridique de Cisco est visiblement excédé par les propos d'un responsable américain de Huawei, affirmant que Cisco se serait désisté après qu'« aucune infraction » n'a finalement été trouvée dans le code source incriminé, qui venait en réalité « d'une tierce partie » et était « librement accessible sur Internet ». Fait très inhabituel et absolument pas diplomatique, le directeur juridique publie quelques extraits du rapport secret d'expertise concluant à l'appropriation frauduleuse[19], et invite crânement Huawei à publier l'intégralité du document. Le groupe de Shenzhen n'en fera rien. Et, bien que les dirigeants de Huawei afficheront par la suite une sérénité de façade sur la crise déclenchée par Cisco, il fait peu de doute que le groupe a été très affecté par l'affaire. Ren Zhengfei songera même en 2003… à vendre son entreprise.

Ping-pong et chemises à fleurs

C'est une photo extraordinaire, publiée par le *Financial Times* en 2019[20]. Ren Zhengfei marche le long de l'océan, sur une plage de sable fin, visiblement décontracté. Il porte une large chemise à manches courtes, dont le tissu bleu clair est égayé par de grands poissons exotiques jaunes, et un short assorti. Le cliché date de la fin 2003, le patron de Huawei n'a pas encore soixante ans. Plus que cet accoutrement, c'est l'homme qui se tient à ses côtés, lui-même en short-tee-shirt, qui fait l'intérêt du document. Il s'agit de Mike Zafirovski, alors numéro 2 de Motorola. Si les deux concurrents sont réunis sur les rivages paradisiaques de l'île de Hainan, au sud de la Chine, c'est parce que l'Américain est sur le point de racheter

Huawei, pour plus de 7 milliards de dollars. Face aux obstacles américains – et alors que, comme le confessera Ren Zhengfei lui-même en 2019 dans une interview à Bloomberg TV : « Nous avions encore peur des États-Unis[21] » –, les dirigeants à Shenzhen sont prêts à renoncer et céder les rênes de l'entreprise à un grand concurrent occidental.

L'opération avortée restera un secret pendant quinze ans. Mais à l'époque, les deux dirigeants ne sont pas loin de l'annoncer au monde. « Leur numéro 2, Mike Zafirovski, avait tout négocié avec nous, les documents avaient tous été signés. En attendant l'accord définitif, on a tous mis des vêtements à fleurs, couru et joué au ping-pong sur la plage[22] », racontera Ren Zhengfei en 2019. Zafirovski plaisante sur sa jeunesse communiste – il a grandi à Skopje, en ex-Yougoslavie – et prend soin de laisser Ren gagner au ping-pong. Tout le monde se félicite de l'heureuse issue qui se dessine. Mais si c'est le numéro 2 de Motorola qui mène les discussions, c'est parce que le poste de directeur général est quasi vacant depuis que Christopher Galvin a annoncé sa démission trois mois plus tôt. Le petit-fils du fondateur de Motorola n'est encore en poste que le temps que le conseil d'administration lui trouve un successeur. Mike Zafirovski est sur les rangs, mais c'est le pétulant Ed Zander – surnommé « Fast Eddie » –, avec sa gouaille de Brooklyn et sa réputation de génie du marketing, qui est finalement nommé le 17 décembre 2003… quelques jours avant la photo sur la plage de Hainan. Une des premières décisions du nouveau patron sera d'annuler le rachat prévu de Huawei, jugé trop cher pour une entreprise étrangère peu connue. Ce n'était sans doute pas la meilleure de sa carrière. « Des années plus tard, quand j'ai rencontré le patron d'Ericsson, il m'a dit que Mike avait pleuré en parlant de ce qui s'était passé[23] », racontera Ren Zhengfei.

Cette transaction aurait pu changer la face du monde. En rachetant son rival, Motorola serait devenu le premier équipementier de Chine et n'aurait peut-être pas périclité. Surtout, Huawei serait devenu américain. Ren Zhengfei lui-même était prêt à se reconvertir « dans le tourisme ou les tracteurs[24] ». Écrire une uchronie en partant du rachat de Huawei en 2003 ouvre une infinité de possibles. Une seule chose est certaine : le rapport de force technologique entre la Chine et les États-Unis, qui structure l'antagonisme des deux superpuissances en 2020, n'aurait pas été le même. Au lieu de cela, Huawei prendra la résolution de poursuivre sa « conquête de l'Est » et de préparer l'inévitable affrontement à venir. Le groupe de Shenzhen est parfaitement conscient qu'il va prendre des coups. Ils ne tarderont pas à pleuvoir.

Les taupes

Il n'est pas rare, dans le monde des technologies, que des conflits sur la propriété intellectuelle se retrouvent devant les tribunaux et prennent des proportions gigantesques. Ainsi, au printemps 2019, après deux ans d'une bataille judiciaire sans merci, et pour échapper à la perspective d'une interdiction des ventes de certains iPhone en Allemagne et en Chine, Apple s'est résolu à payer la somme colossale de 4,5 milliards de dollars en arriérés de droits sur les brevets de Qualcomm. Comme ses pairs, Huawei défend chèrement sa propriété – souvent avec succès. En 2018, le groupe a par exemple fait condamner Samsung – le premier constructeur de téléphones au monde – pour avoir enfreint deux de ses brevets liés à la 4G. Dans une industrie où l'innovation est permanente et susceptible de faire

vaciller tous les trônes, tous les acteurs sont procéduriers et rodés à ces procès à rallonge.

Ce qui est moins fréquent en revanche, c'est qu'une grande entreprise soit nommément accusée de plagiats aussi grossiers que Huawei dans l'affaire de Cisco. Pire, les années suivantes, les plaintes dans la même veine se succèdent à l'encontre du groupe. Et malgré l'absence de condamnation, la réputation du Chinois ne s'en remettra jamais tout à fait. À peine a-t-il apaisé le courroux de Cisco que Huawei accuse les foudres de Fujitsu. Dans un courrier adressé à Ren Zhengfei[25], son directeur juridique se plaint du comportement ahurissant d'un salarié du groupe. Sur un salon professionnel de Chicago, celui-ci a été surpris en pleine nuit par les équipes de sécurité. Muni d'un appareil photo, Yi Bin Zhu photographiait les circuits imprimés d'un équipement mobile du constructeur japonais, d'une valeur d'un million de dollars, dont il avait au préalable soulevé l'étui protecteur. En plus de la carte mémoire de l'appareil, les agents confisquent un carnet de notes rempli de croquis sur des centraux téléphoniques d'AT&T et une liste d'entreprises et de produits concurrents. Sur son badge, on peut lire « Weihua » – le nom inversé du groupe de Shenzhen. L'indélicat est licencié. Huawei précisera qu'il s'agissait d'un « ingénieur junior qui n'avait jamais voyagé aux États-Unis auparavant », et dont « les actions ne reflètent pas la culture ou les valeurs de Huawei ». Certains de ses concurrents peuvent légitimement émettre des doutes. C'est le cas par exemple de Motorola, qui portera plainte à son tour en 2010 contre son rival chinois, l'accusant d'avoir recruté une poignée de taupes dans ses équipes[26]. L'un de ces supposés infiltrés, Shaowei Pan, qui travaillait depuis 1994 pour la firme américaine, aurait rencontré Ren Zhengfei en personne en 2001, avant de lui transmettre de la documentation commerciale et technique. Bien qu'il ait tenté d'effacer le contenu de

son ordinateur avant sa saisie, un e-mail envoyé depuis sa boîte privée y aurait été retrouvé avec, en pièce jointe, les « détails demandés » sur une technologie d'antenne ultralégère développée par Motorola. Un autre de ces salariés indélicats, Hanjuan Jin, aurait accédé pendant des années aux ordinateurs de Motorola depuis l'extérieur. Jusqu'à ce qu'un soir de 2007, elle télécharge et imprime une foule de documents confidentiels estampillés « Motorola » avant de prendre le chemin de l'aéroport de Chicago. La douane l'arrêtera avant qu'elle ne prenne place dans un vol pour Pékin, avec ce fabuleux butin et 30 000 dollars en liquide. Cette affaire des taupes, assez extraordinaire, sera curieusement abandonnée par Motorola en 2011[27]. Il ne faut sans doute pas y voir un acte de charité, mais plutôt de *Realpolitik*. À cette époque, le groupe américain attend impatiemment de pouvoir vendre son activité d'équipementier mobile à Nokia. Le Finlandais lui en offre près d'un milliard de dollars[28]. Mais l'opération tarde à se concrétiser, car elle est attaquée en justice par Huawei et scrutée de près par les autorités de concurrence chinoises. Début 2011, le premier retirera sa plainte et les secondes donneront leur feu vert. Plus personne n'entendra parler des taupes de Motorola. Dans le monde des affaires, il faut savoir faire des concessions. Et ce n'est pas comme si les histoires de carambouille et de chapardage manquaient dans le monde de la tech. Celle qui va secouer T-Mobile en 2012 n'a toujours pas fini de faire travailler la justice américaine, huit ans après les faits.

Tappy le robot

Les smartphones sont des objets fragiles. Il n'y a guère que les vendeurs de coques de protection à s'en féliciter. Pour les

consommateurs, c'est le risque d'être inopinément privés de leur indispensable assistant numérique. Et pour les opérateurs – qui restent les principaux distributeurs de terminaux, qu'ils subventionnent pour fidéliser leurs clients –, les voir tomber en panne est un énorme problème en termes de logistique et d'image. Pour limiter les retours de clients mécontents, l'opérateur américain T-Mobile a une solution. Il se fait envoyer les appareils par ses fournisseurs, en amont de leur mise sur le marché, et il les malmène dans une salle de torture spécialement conçue. Là, il peut vérifier leur résistance aux chocs répétés ou aux séjours inopinés dans l'eau, mesurer la qualité du signal audio dans des environnements bruyants ou la bonne réception des ondes radio quelle que soit la position du téléphone. En 2006, les équipes de T-Mobile ont développé un robot d'un nouveau genre pour participer à ce supplice. Répondant au petit nom de Tappy, il se présente sous la forme d'un bras mécanique articulé. Son rôle est, des heures durant, de simuler l'utilisation d'un écran tactile et de vérifier que, même à haute dose, l'interface continue de répondre. Le robot réalise en parallèle des mesures techniques, comme la rapidité à laquelle s'use la batterie pendant ces tests. Tappy est un bourreau efficace. T-Mobile est plus que satisfait de ses performances. Il laisse ses fournisseurs accéder au local fermé et protégé où il soumet leurs smartphones à la question, mais seulement à certaines personnes dûment autorisées. Pas moyen que la technologie de Tappy se retrouve dans la nature et profite à des concurrents.

Huawei, dont certains salariés disposent d'un badge pour accéder à Tappy, est très intéressé par le robot. Un peu trop même, au goût de T-Mobile, qui portera plainte contre le groupe chinois en 2014[29]. Selon l'opérateur, Huawei voulait développer son propre robot pour effectuer des tâches similaires directement dans ses usines de

Shenzhen. Le groupe avait même proposé à T-Mobile de lui acheter ou de lui louer les droits de la technologie. Mais l'Américain avait poliment décliné, au motif que Huawei travaillait aussi pour certains de ses concurrents directs, et qu'il n'était pas question qu'ils profitent indirectement du savoir-faire de Tappy. Jusque-là, tout allait bien. Mais, à en croire T-Mobile, son fournisseur ne l'a pas entendu de cette oreille. Après le refus poli des Américains, les ingénieurs du siège, à Shenzhen, se sont mis à presser leur filiale aux États-Unis de leur fournir des informations techniques sur les composants matériels et logiciels de l'automate. Bien embêtés, les salariés américains ne pouvaient que répondre par la négative et leur signifier que leurs questions répétées avaient déjà éveillé les soupçons de T-Mobile. Une caméra de surveillance avait même été installée dans la salle de Tappy. Au printemps 2013, c'est donc un employé de la maison mère qui débarque à Bellevue, dans la banlieue de Seattle, pour tenter de découvrir les secrets du robot. Le plus simplement du monde, il emprunte le badge de ses collègues autorisés, et pénètre dans les locaux pour photographier et mesurer l'engin. À deux reprises, sa présence est détectée par les équipes de T-Mobile, qui lui demandent de quitter les lieux. Fâché de la mésaventure, l'opérateur demande alors aux employés accrédités de rendre leur badge. Tentant le tout pour le tout, l'un d'entre eux retourne alors dans les salles de test et fourre purement et simplement le bras articulé de Tappy dans sa sacoche d'ordinateur avant de s'en aller. Le technicien n'est clairement pas un professionnel de la rapine et le vol ne tardera pas à être découvert. Après avoir initialement nié, l'employé évoquera une « erreur » et retournera l'objet de son larcin. Là encore, Huawei regrettera les agissements de ses deux salariés et licenciera ces brebis galeuses, qui ne sauraient représenter les dizaines de milliers d'employés du groupe. L'affaire ira néanmoins à son terme devant la

justice fédérale, et Huawei sera condamné en 2017 par un jury de Seattle pour violation de contrat et détournement de secrets industriels. Pour les jurés, cette dernière infraction n'était toutefois pas « délibérée et malveillante » et l'amende finale de 4,8 millions de dollars sera sensiblement inférieure à ce que demandait T-Mobile[30].

L'affaire Tappy aurait pu se refermer là. Une incroyable histoire de pieds nickelés qui débouche sur une sanction pécuniaire et sur la perte d'un gros client (T-Mobile cessera de distribuer les smartphones Huawei). D'autant que ce robot reste « un doigt en caoutchouc qui tape sur un écran de smartphone. Ce n'est pas sorcier », pointera William Plummer, un ancien responsable de Huawei USA, dans une interview donnée en 2019 à un journal de Seattle[31]. Quoi qu'il en soit, le verdict du jury a été rendu, la justice est passée. Mais deux ans plus tard, en janvier 2019, Tappy s'invite à nouveau dans l'actualité, quand les autorités fédérales dévoilent une autre plainte contre Huawei – sur les mêmes faits, mais avec une précision très dommageable pour le groupe. Washington avance dans son dossier d'accusation que, loin d'être un incident « isolé » comme le prétend Huawei, la conduite de ses deux salariés s'inscrit dans une politique institutionnalisée. Un « programme de bonus pour récompenser les employés ayant obtenu des informations confidentielles des concurrents » aurait été lancé en 2013, avec un site interne pour recueillir ces bons tuyaux, et même une adresse e-mail spéciale en huawei.com où envoyer un message chiffré pour les informations les plus sensibles. À la prime mensuelle attribuée par un « groupe de gestion de la concurrence » aux meilleurs fouineurs, s'ajoutaient, selon Washington, des primes bisannuelles aux équipes régionales les plus efficaces dans la collecte de renseignements.

Huawei a réfuté catégoriquement l'existence d'un tel programme. Comme souvent, les États-Unis n'ont mis à disposition du public

aucune preuve tangible pour appuyer leurs graves accusations, laissant le groupe chinois se débrouiller pour éteindre l'incendie médiatique qui, à chaque nouvelle attaque, repart de plus belle. Depuis vingt ans, Huawei répète qu'il est la victime d'une campagne calomnieuse alors même qu'il est un acteur central et respectueux de la recherche mondiale – commercialisant ses dizaines de milliers de brevets et réglant, rubis sur l'ongle, des centaines de millions de dollars de royalties pour utiliser ceux de ses partenaires américains. Rien n'y fait. C'est comme une vieille tache qui refuserait de partir et qui alimente tous les fantasmes – au point d'autoriser Travis Russell, le directeur de la cybersécurité d'Oracle, à faire en 2019, avant l'ouverture du Mobile World Congress de Barcelone, une déclaration hallucinante. « Je vais passer la semaine entière à chasser les employés de Huawei de mon stand, assure le dirigeant. Parce qu'ils sont payés 5 dollars pour chaque photo qu'ils prennent[32]. »

Des bâtons dans les roues

Le plus gros problème pour Huawei, en ce début de siècle, n'est pourtant pas la réputation sulfureuse que lui valent ces affaires à répétition, parfois montées en épingle à partir de peu de choses, souvent sans preuves concrètes à l'appui. Ses démêlés officiels et officieux avec les autorités américaines n'empêchent absolument pas la société de croître à très grande vitesse, de la Russie à l'Amérique du Sud en passant par l'Europe et l'Afrique. En revanche, ils obèrent son développement aux États-Unis – le premier marché et le phare technologique du monde.

Pour y remédier, une autre tactique va être tentée. Le mérite en revient à 3Com, un concurrent américain de Cisco, fleuron oublié de

la tech des années 1990, dont l'aventure est retracée dans un ouvrage récent, *3Com, la saga jamais racontée de la start-up de la Silicon Valley qui a aidé à la naissance d'Internet – avant de perdre le ballon*[33]. Après l'éclatement de la bulle Internet, ses dirigeants ont un plan pour se relancer. Ils veulent miser sur la Chine et cherchent un partenaire local. Ce sera Huawei. Le P.-D.G., Bruce Claflin, propose d'aider son concurrent asiatique à « surmonter le problème de marque de Huawei en utilisant 3Com ». Lui y gagnerait un accès au marché chinois et aux capacités de R&D du groupe de Shenzhen. Chaque ingénieur en Chine coûte alors quatre fois moins cher qu'aux États-Unis, selon Bruce Claflin. Après un rendez-vous de quatre heures avec Ren Zhengfei, l'affaire est entendue. Une joint-venture, du nom de H3C, est créée, dont Huawei possède 51 % du capital et 3Com 49 %. L'entente n'est, bien sûr, pas du goût de John Chambers. Flairant la menace, le patron de Cisco se serait même déplacé en personne à Shenzhen pour faire dérailler l'opération, proposant à Ren Zhengfei de le racheter pour 200 millions de dollars[34]. Après le refus de l'entrepreneur chinois, Cisco ne mettra pas longtemps à déclencher les hostilités en justice. 3Com, qui a fait sa propre analyse des infractions reprochées à son partenaire – et les juge bien moins graves que ce que prétend Cisco –, aidera Huawei à parer les coups jusqu'à l'abandon de la plainte en 2004.

La collaboration 3Com-Huawei est fructueuse. Au point qu'après que l'Américain a racheté à son partenaire chinois sa participation pour 882 millions de dollars en 2007, le groupe de Shenzhen tente carrément – en appui de la société d'investissement Bain Capital – de racheter tout 3Com pour un peu plus de 2 milliards de dollars. Bain n'est pas qu'un gros poisson de la finance américaine. C'est aussi la société de Mitt Romney, l'austère mormon qui s'est fait élire gouverneur du Massachusetts et ira jusqu'à être le candidat du Parti

républicain à la présidentielle de 2012 face à Barack Obama. Las, ces prestigieuses références ne suffiront pas. L'opération a éveillé les vigies du CFIUS – le Comité pour l'investissement étranger aux États-Unis, un organisme méconnu qui regroupe une dizaine d'agences fédérales et examine ce type de transactions afin de déterminer s'il existe un risque pour la sécurité nationale. Au grand dam de Huawei, leur réponse sera inflexiblement : « Non[35] », pas question que le Chinois s'invite au capital de l'équipementier californien. Bain Capital jettera l'éponge – et c'est Hewlett-Packard qui avalera 3Com l'année suivante.

Régulièrement accusé de servir de paravent à une politique protectionniste, le mandat du CFIUS est pourtant strictement limité aux questions de sécurité. Dans le cas de 3Com, ce sont d'ailleurs ses contrats avec l'armée américaine qui alarment Washington, inquiet à l'idée qu'un groupe chinois se trouve en mesure de trafiquer les équipements et logiciels utilisés par ses forces armées[36]. Quelle qu'en soit la justification, la fin de non-recevoir opposée par le CFIUS à Bain et Huawei constitue un tournant majeur. Pour la première fois, ce ne sont plus des rumeurs et des procès qui viennent gêner le champion chinois des télécoms. L'administration américaine est intervenue pour lui barrer le chemin. Et elle ne se privera pas de le faire, encore et encore.

Des terres contre la paix

La porte qui reste désespérément fermée à Huawei est celle des grands opérateurs télécoms américains. Le groupe chinois a bien réussi à séduire des acteurs de moindre envergure, comme ClearWire ou Cox Communications. Mais la stratégie du « contournement des

villes par les campagnes », qui lui a si bien réussi jusqu'alors, ne fonctionne pas aux États-Unis. Au début des années 2010, les quatre géants qui règnent en maîtres sur le marché – AT&T, Verizon, Sprint et T-Mobile – continuent de faire l'impasse sur le matériel chinois. Ce sont d'ailleurs les seuls, parmi les 40 plus gros opérateurs du monde, à ne pas être en affaires avec Huawei. Le groupe de Shenzhen espère que le passage de la 3G à la 4G sera l'occasion de mettre enfin le pied dans la porte. Signe de cette ambition, Huawei a inauguré de nouveaux locaux en novembre 2009 à Plano – la petite ville voisine de Dallas et du siège d'AT&T où il a posé ses valises huit ans plus tôt. L'immeuble de cinq étages, où il loue maintenant près de 10 000 m^2, n'est qu'à une quinzaine de kilomètres de cette implantation historique, de l'autre côté des greens de golf du Gleneagles Country Club. D'ici trois ans, Huawei a prévu d'y augmenter ses effectifs de moitié pour atteindre 600 personnes. Dans un discours préparé pour l'occasion, le maire de Plano se félicite de cette expansion, qui « ouvre la voie à la croissance de Huawei aux États-Unis[37] ». Il faut dire que la ville vient de voter une subvention de 700 000 dollars à ce grand pourvoyeur d'emplois. Reste à décrocher les contrats.

Fin 2009, AT&T commence à sonder les équipementiers pour la mise à niveau de son réseau. Des centaines de millions de dollars sont à la clé. Et, comme l'expliquera un article du *Washington Post* début 2010, la direction du premier opérateur américain n'est pas insensible au charme des antennes Huawei[38]. Devenu deuxième équipementier mondial, le Chinois n'a plus à faire sa réputation de fournisseur de qualité, imbattable sur les prix et le service client. AT&T se verrait bien lui confier une partie de la commande. Du moins jusqu'à ce que les dirigeants de l'opérateur reçoivent un appel de la NSA[39]. Le message des espions américains est très clair. Si AT&T veut rester un fournisseur de l'administration américaine – de très nombreux

services officiels utilisent les réseaux de l'opérateur –, il serait avisé de ne pas s'équiper de matériel chinois. Les agents secrets expliquent à AT&T redouter que des *backdoors* ne permettent aux services chinois de se servir du matériel Huawei en cachette. L'agence ne dit pas qu'au même moment, ses services sont engagés dans l'opération « Shotgiant » pour infiltrer les réseaux de Huawei et implanter leurs propres *backdoors*[*1]. Soit que l'argument sécuritaire ait porté, soit que la menace de perdre les juteux contrats de l'administration ait fait son effet, AT&T change rapidement son fusil d'épaule. Début février 2010, il annonce les vainqueurs de son appel d'offres pour la 4G. Ce sont le suédois Ericsson et le français Alcatel-Lucent[40]. Le même duo occidental est retenu par Verizon.

Les deux plus grosses opportunités américaines se sont envolées. Mais celle sur laquelle Huawei, plus raisonnable, a tout misé, c'est le passage à la 4G de Sprint. Le numéro 3 du marché est à la peine. Le nombre de ses abonnés diminue sans discontinuer depuis deux ans. Il a besoin de muscler son réseau pour enrayer cette spirale et a prévu d'investir plus de 5 milliards de dollars dans un programme baptisé « Network Vision ». Pour obtenir ce contrat, Huawei va sortir le grand jeu. Quelques mois plus tôt, il a débauché pour sa filiale américaine le directeur technique de BT, Matt Bross, qui supervisait plusieurs années auparavant « 21st Century Network », le contrat britannique à 10 milliards de dollars ayant servi de tremplin à Huawei en Europe. Sa mission est désormais de décrocher son équivalent Outre-Atlantique – « Network Vision ».

Pour l'aider, Huawei a mandaté The Cohen Group. Fondé par un ancien secrétaire à la Défense, le groupe de consultants de haut vol doit trouver des solutions pour surmonter les réticences de l'administration américaine. Sa proposition, selon le *Washington Post*, est radicale. Elle consiste à séparer structurellement la filiale

américaine, en en faisant une entreprise américaine dotée de son propre conseil d'administration qui ne serait plus contrôlée par sa maison mère chinoise[41]. En parallèle de ce travail, Huawei a mis un deuxième fer au feu, en la personne de William Owens. Ce fin et raide officier sous-marinier, à la mise aussi impeccable que sa raie sur le côté, n'est pas seulement un vétéran du Vietnam, du Golfe et des Balkans. Le natif des rudes plaines du Dakota du Nord a surtout grimpé quatre à quatre les échelons jusqu'à devenir, sous Bill Clinton, le numéro 2 des forces armées américaines, supervisant plus de 1,5 million de soldats. Après avoir quitté l'uniforme, ce militaire technophile a également été patron de Nortel, le fleuron canadien des télécoms. On peut difficilement rêver mieux comme ambassadeur. Pour accompagner Huawei dans sa quête du contrat Sprint, l'amiral en retraite a monté une société *ad hoc*, Amerilink, et recruté une véritable *dream team* du lobbying, qui comprend notamment un ancien patron de la Banque mondiale, un ancien chef de la majorité au Congrès américain ou encore un ex-secrétaire adjoint à la Défense[42]. Amerilink recrute aussi plusieurs cadres de Sprint et s'établit à Overland Park. La deuxième ville du Kansas a la particularité d'accueillir le siège… de Sprint. Au-delà d'aligner une liste de CV impressionnante, Amerilink a un plan. La firme compte proposer aux autorités américaines d'être un tiers certificateur, c'est-à-dire de faire vérifier le matériel et les produits de Huawei avant qu'ils ne soient déployés sur le territoire américain. L'idée est peu ou prou celle de The Cell, le labo des services secrets britanniques qui dissèque les produits de Huawei, si ce n'est qu'elle repose sur des acteurs privés.

Cette débauche de moyens a-t-elle éveillé plus de suspicions qu'elle n'en a apaisé ? Les équipes de The Cohen Group et d'Amerilink se sont-elles torpillées l'une l'autre ? Ou est-ce le coup de

téléphone passé par le secrétaire au Commerce au patron de Sprint peu avant que la décision ne soit prise qui a fait pencher la balance ? Toujours est-il que le 6 décembre, quand l'opérateur révèle le nom des trois fournisseurs retenus, Huawei ne fait pas partie de la liste. Il a été évincé pour des « raisons de sécurité nationale », assurent des proches du dossier au *Wall Street Journal*[43]. Adieu « Vision Network », adieu les 5 milliards de dollars et adieu le rêve de percée historique sur le marché américain.

À la déception, Huawei n'ajoute pourtant pas la rancœur. Le groupe semble accepter chaque déconvenue avec philosophie. Régulièrement, ses dirigeants expliquent même qu'ils n'ont pas besoin du marché américain ou qu'ils sont heureux que leurs concurrents remportent de gros contrats. Ren Zhengfei porte le même message avec constance, en invitant à s'inspirer du Premier ministre israélien assassiné Yitzhak Rabin – à qui le patron voue un grand respect pour avoir accepté d'« échanger des terres contre la paix[44] ».

Un rapport au vitriol

Pourtant les rebuffades de l'administration américaine sont cruelles. Début 2011, un nouveau cap est franchi. Ce n'est plus que l'on interdit à Huawei – plus ou moins subtilement – de signer des contrats. Cette fois, les autorités lui demandent carrément d'annuler une transaction et de rétrocéder des actifs légalement acquis. Neuf mois plus tôt, c'est tout à fait légitimement que le groupe chinois s'est porté acquéreur, pour 2 millions de dollars, de certains brevets de 3Leaf, une start-up californienne ayant fait faillite. Huawei expliquera même avoir soumis le dossier au BIS, le Bureau de l'industrie et de la sécurité chargé pour le Département du commerce américain de

vérifier le respect des règles en matière d'exportation de technologies. Les fonctionnaires donneront leur feu vert. Mais c'était sans compter sur le fameux Comité fédéral qui avait déjà mis son nez dans la proposition de rachat de 3Com trois ans plus tôt. Une nouvelle fois, c'est la sécurité nationale qui sert de justificatif idéal. « Le 11 février 2011, le CFIUS a officiellement signalé qu'il recommandait que Huawei défasse l'opération 3Leaf », explique le groupe chinois dans un e-mail au *Wall Street Journal*, ajoutant avoir « décliné la proposition »[45]. Une semaine plus tard, Huawei fait pourtant machine arrière. Le vif débat que suscite l'affaire dans l'opinion n'est pas à son avantage. Le groupe chinois préfère renoncer à ses brevets et tenter, une bonne fois pour toutes, de s'expliquer. Il le fera par le biais d'une lettre publique de six pages, signée de Ken Hu, le vice-président tournant de Huawei[46].

Dans ce courrier d'anthologie, le dirigeant loue les États-Unis et ce qu'ils représentent. « Les valeurs de la démocratie, de la liberté, de l'État de droit et des droits de l'homme aux États-Unis sont celles que Huawei respecte, défend et pratique », écrit Ken Hu, qui cite aussi Obama et Lincoln. Cette ode à l'Amérique accompagne une longue tentative d'explication, pour balayer dix ans de critiques et de soupçons – sur les connexions rapprochées avec l'armée chinoise, les violations de propriété intellectuelle, le financement par le gouvernement chinois ou les menaces pour la sécurité nationale des États-Unis. Tout y passe. Et tout est méthodiquement démenti. Dans un exercice auquel l'entreprise ne s'est jamais risquée, Ken Hu donne des éléments factuels sur le passé de Ren Zhengfei, mais aussi des chiffres inédits sur les lignes de crédit accordées à Huawei ou encore des précisions sur l'ampleur de ses investissements en R&D aux États-Unis comme déposant de brevet et comme utilisateur de licences. Le vice-président tournant de Huawei répète à plusieurs reprises un

message – qui conclut d'ailleurs sa lettre : il espère que les États-Unis mèneront une enquête officielle sur son groupe, afin de « prouver que Huawei est une institution commerciale et rien de plus ».

Son vœu sera exaucé, mais Ken Hu regrettera sans doute de l'avoir formulé. Un mois après la parution de sa lettre, en novembre 2011, une enquête est ouverte par le Congrès américain – et plus spécifiquement son comité spécial permanent sur le renseignement – sur « les problèmes de sécurité nationale posés par les entreprises chinoises de télécommunications Huawei et ZTE[47] ». Pendant un an, les auditions de témoins et les réquisitions de documents s'enchaînent. Et quand le rapport du Congrès est finalement rendu public le 8 octobre 2012, Huawei ne peut que déplorer son contenu. C'est un réquisitoire violent contre le groupe de Shenzhen et son compatriote ZTE.

Mike Rogers et Dutch Ruppersberger, les deux élus américains qui ont conduit l'enquête, sont catégoriques. Huawei et ZTE n'ont pas coopéré pleinement et ont laissé l'essentiel de leurs questions sans réponse. Et ces interrogations sont les mêmes qui taraudent les services secrets et l'administration américaine depuis plus d'une décennie : qui est réellement Ren Zhengfei ? Quels sont les liens de son groupe avec le gouvernement chinois, le parti communiste et l'Armée populaire de libération ? Qui contrôle et qui finance Huawei ? Le groupe respecte-t-il les sanctions internationales et américaines visant l'Iran ? Sur 50 pages, le rapport ne fait que constater l'absence d'éléments probants apportés par les deux entreprises pour apaiser leurs craintes.

Malgré des heures d'entretien avec les dirigeants de Huawei et de ZTE, les parlementaires américains sont restés sur leur faim. Ils se vengent dans leurs conclusions, en recommandant une vigilance accrue des services de sécurité, le blocage de toute transaction

impliquant Huawei ou ZTE par le CFIUS, et en invitant les acteurs privés, notamment les opérateurs télécoms, à choisir d'autres fournisseurs. Pour Huawei, ça aurait difficilement pu être pire. La seule chose que Rogers et Ruppersberger se sont abstenus de réprouver, ce sont leurs ventes de smartphones au grand public américain. Pour un rapport qui, comme le dira cruellement l'agence Reuters, « regorge de soupçons et manque de preuves[48] », le résultat paraît presque disproportionné. Dans un post de blog quelques mois plus tard, alors que les révélations de Snowden défraient la chronique, John Suffolk – le responsable de la cybersécurité de Huawei et ancien directeur informatique de la Couronne britannique – ne pourra s'empêcher un trait sarcastique : « À partir d'une absence de preuve […], le Congrès américain a dit que Huawei ne devrait pas être autorisé aux États-Unis, alors à partir de ces révélations […] tous les gouvernements devraient-ils bannir les entreprises technologiques américaines[49] ? »

Ce 8 octobre 2012, ce n'est pas qu'une exclusion du marché américain de Huawei et ZTE qui a été, sinon inscrite dans la loi, du moins fortement recommandée par le législateur. C'est aussi une gifle diplomatique que les États-Unis ont pris le risque d'infliger à Pékin – moins de cinq mois avant l'intronisation de Xi Jinping comme nouveau président de la République populaire de Chine. L'affront ne sera pas oublié. Rétrospectivement, il apparaît comme un premier signe fort de la fracture qui va se dessiner entre les deux blocs. La 5G, véritable détonateur de cette crise en préparation, est déjà dans les laboratoires en 2012. Il ne manque que quelques années pour qu'elle sorte des salles blanches, poussant les États-Unis à ne plus limiter leurs attaques contre Huawei à leur seul territoire national. Bientôt, le conflit sera mondial. Le 1er décembre 2018, il fera même sa première victime. C'est une femme de quarante-six ans qui ne se

doute encore de rien. Elle est pour l'heure tranquillement assoupie, en classe affaires, sur un vol de la Cathay Pacific à destination de Vancouver.

---

*1. Voir chap. IV, p. 97.

CHAPITRE VI

Le *Blitzkrieg* de Washington

À partir de 2018, tout s'accélère. L'orage qui grondait depuis tant d'années à Washington éclate soudain et la foudre s'abat sur Huawei. Le groupe est attaqué comme aucune entreprise de cette taille ne l'a jamais été. De même que l'avenir de sa directrice financière, placée en résidence surveillée au Canada, celui de Huawei devient soudain très incertain.

La case prison

Il n'est pas encore 11 h 30 quand le pilote du Boeing 777 aperçoit la piste. Une légère pluie assombrit le tarmac de l'aéroport de Vancouver, ce qui n'a rien d'inhabituel pour un début de mois de décembre sur la façade pacifique du Canada. Le vol CX838, en provenance de Hong Kong, est légèrement en avance – ce dont ne peuvent que se féliciter les passagers, après plus de onze heures à bord. Bientôt, une file se forme et franchit la porte de l'avion, sous l'œil des agents de la douane canadienne. Ce n'est pas un banal contrôle. Les fonctionnaires recherchent une femme de quarante-six

ans, dont on leur a communiqué deux photos d'identité et un numéro de passeport hongkongais. Repérée, elle est emmenée par les agents au contrôle des bagages. Elle leur remet son matériel électronique : un MacBook, un iPad, un iPhone blanc et un smartphone rouge de marque Huawei – dont elle communique les codes de déverrouillage aux douaniers. Son interrogatoire dure près de trois heures. Et ce n'est qu'en début d'après-midi, ce 1er décembre 2018, que des officiers de la police montée canadienne finissent par se présenter. Ils expliquent à la voyageuse qu'elle fait l'objet d'un mandat d'arrêt. Les États-Unis demandent son extradition pour répondre de graves accusations liées à sa fonction. La femme s'appelle Meng Wanzhou. Elle est la directrice financière et la vice-présidente de Huawei. Elle est aussi la fille aînée de son fondateur, Ren Zhengfei. C'est d'ailleurs pour retrouver ce dernier à une conférence en Argentine que la dirigeante a pris un vol à Hong Kong, avec deux changements, à Vancouver puis Mexico. Elle n'avait pas prévu que sa première escale allait durer des années et commencer par un séjour en prison.

Cette arrestation est une accélération dramatique dans la confrontation entre Huawei et les États-Unis qui court depuis bientôt vingt ans. C'est aussi un moment incontournable de la guerre technologique entre l'Amérique et la Chine, qui ne va pas tarder à déchirer la planète. Symboliquement, c'est le premier coup de feu qui survient après des années de tension et qui prélude une violente réaction en chaîne. Toutes proportions gardées, le meilleur parallèle qui vienne à l'esprit est l'attentat de Sarajevo de juin 1914, qui précipitera le jeu des alliances européennes et, *in fine*, la guerre. Mais ce samedi après-midi, personne n'a encore conscience de la gravité de la situation. Meng Wanzhou n'a pas réussi à joindre un avocat de Huawei, ni son consulat[1]. Shenzhen est à 10 000 km de Vancouver et le soleil s'y lève à peine. Quant à Xi Jinping et Donald Trump, ils sont

d'excellente humeur. Les présidents américain et chinois sont réunis, à l'occasion du G20, à Buenos Aires – précisément la ville que comptait rejoindre Meng Wanzhou – et annoncent au monde une trêve dans le conflit commercial qui oppose leurs deux pays depuis six mois, à grands coups de relèvements de droits de douane et de mesures de rétorsion. La poignée de mains entre Xi et Trump – premier épisode de détente depuis l'élection du tempétueux locataire de la Maison-Blanche – rassure les agriculteurs américains et les marchés financiers. Leur soulagement serait peut-être moindre s'ils savaient ce qui se trame au même moment, à 11 000 km plus au nord.

Menottée par la police fédérale, Meng Wanzhou est finalement conduite au centre correctionnel pour femmes Alouette, à une soixantaine de kilomètres à l'est de l'aéroport. Situés au milieu d'une forêt d'énormes conifères, ses baraquements entourés de barbelés n'ont très certainement jamais accueilli la dirigeante d'une entreprise de 190 000 personnes et de 100 milliards de dollars de chiffre d'affaires. Derrière les lourdes portes métalliques des cellules, les détenues sont plus souvent accusées de violences ou de possession de drogue que d'avoir menti à de grandes banques internationales au sujet de violations des sanctions américaines contre l'Iran. Car c'est pour répondre de ce supposé crime que les États-Unis ont demandé au Canada d'arrêter et de déporter Meng Wanzhou sur leur sol. Ironiquement, le centre correctionnel Alouette est plus proche encore de la frontière américaine que de l'aéroport de Vancouver. Mais une brochette d'avocats parmi les meilleurs du Canada va tout faire pour éviter que leur cliente ne soit emmenée de l'autre côté de cette ligne de démarcation juridique, et dans un premier temps, qu'elle ne croupisse derrière des barreaux.

Le contraste est forcément immense entre le centre correctionnel et les palaces où Meng Wanzhou mène d'ordinaire son existence de femme d'affaires internationale et de fille de milliardaire. Pour ne rien arranger, la directrice financière de Huawei a une santé vacillante – comme le souligneront ses avocats devant les juges de la Cour suprême de Colombie-Britannique[2]. Elle souffre d'hypertension et a dû être opérée d'un cancer de la thyroïde en 2011. Le stress de l'arrestation a déjà fait bondir sa pression artérielle au point de lui valoir un passage par le Richmond General Hospital et la vice-présidente de Huawei, dans une déclaration sous serment, affirme être « préoccupée par une détérioration de [s]a santé tandis qu['elle] est incarcérée[3] ». Ce n'est pas l'effroi d'une gosse de riche devant la précarité du système carcéral. Contrairement à sa jeune demi-sœur Annabel Yao – qui valsait une semaine plus tôt au prestigieux Bal des débutantes parisien, dans une robe du créateur J. Mendel –, Meng Wanzhou n'a pas eu une enfance dorée. Née deux ans avant le départ de son père pour l'armée – il reconnaîtra lui-même ne l'avoir vue qu'épisodiquement –, elle est élevée par sa mère, l'ex-garde rouge de Chongqing dont elle a gardé le nom de famille et qui allait, comme le raconte Ren Zhengfei, à la fin des marchés, acheter « des poissons morts et des crevettes pas très fraîches qui coûtaient deux fois rien[4] » pour que l'enfant ait des protéines. Elle a quinze ans quand son père se lance dans les affaires, avec une poignée de dollars et beaucoup de culot ; vingt et un ans quand elle entre elle-même chez Huawei, tout en bas de l'échelle, avant de reprendre des études à l'université des sciences et technologies de Huazhong, d'obtenir son master et de gravir un à un les échelons du groupe familial jusqu'à son poste actuel de directrice financière.

Des millions de caution

Depuis au moins une dizaine d'années toutefois, Meng Wanzhou faisait bien partie d'une toute petite élite des affaires – voyageant sans arrêt d'un bout à l'autre de la planète, parfaitement à l'aise en anglais –, la *lingua franca* du business, côtoyant les puissants et dormant dans les meilleurs hôtels entre deux nuits dans l'avion. Comme beaucoup de Chinois qui voyagent, elle a pris l'habitude d'occidentaliser son nom et se fait fréquemment appeler Sabrina ou Cathy Meng. En plus de quatre appartements à Shenzhen et à Hong Kong, elle en possède trois à Londres et deux maisons à Vancouver, où elle a résidé plusieurs années, obtenu le statut de résidente permanente et un temps scolarisé deux de ses quatre enfants[5]. Fin 2018, tandis que sa demi-sœur termine son cursus à Harvard, l'un des fils de Meng Wanzhou poursuit également sa scolarité aux États-Unis, signe de l'estime dans laquelle elle tient le pays. « Les États-Unis ont donné naissance à la société la plus avancée et à un nombre incalculable d'individus exceptionnels », expliquait-elle en juin 2014, à l'ouverture d'un forum financier organisé par Huawei à New York en présence d'Alan Greenspan, l'ancien président de la Réserve fédérale américaine[6]. « Ces réussites peuvent être attribuées à l'idéalisme et à la détermination du peuple américain et aux systèmes avancés, flexibles, des États-Unis, et – de manière plus importante – à la culture américaine, dans laquelle les individus sont respectés, les innovations encouragées, les échecs tolérés et les droits à la propriété intellectuelle protégés. […] Dans l'avenir, nous continuerons à apprendre des États-Unis ; en réalité ils seront notre professeur pendant encore longtemps. »

Mais, quatre ans après cette vibrante déclaration d'amour, les autorités américaines ont noté chez leur admiratrice une certaine

prise de distance, au moins physique. Alors que Meng Wanzhou se rendait très régulièrement aux États-Unis, elle n'a plus posé le pied sur le sol américain depuis bientôt deux ans. Les enquêteurs la soupçonnent, comme plusieurs autres dirigeants de Huawei, d'éviter soigneusement leur territoire depuis qu'en avril 2017, la filiale américaine du groupe a reçu une citation à comparaître devant un grand jury – signe qu'une enquête criminelle était engagée[7]. Et de fait, l'information est secrète mais depuis le 22 août 2018, un mandat d'arrêt concernant la directrice financière de Huawei a été émis aux États-Unis. Seulement, si Meng Wanzhou continue de snober les États-Unis, il sera difficile de l'appréhender. La Chine, en particulier, n'extrade pas ses ressortissants. La solution la plus simple, puisque la suspecte doit faire escale à Vancouver, est de demander au Canada d'effectuer la basse besogne. Le 30 novembre 2018, un mandat d'arrêt provisoire est envoyé aux autorités canadiennes. Le lendemain, Meng Wanzhou est cueillie par la police montée. Il ne reste aux États-Unis qu'à acquérir la certitude qu'elle sera bien extradée. Pour cela, le procureur américain écrit à la cour de Vancouver pour s'assurer que sa proie restera en prison et ne s'enfuira pas hors de sa portée. Dans son courrier, il établit clairement un lien entre l'absence de voyages aux États-Unis de la Chinoise et une volonté d'échapper à la justice. Le juge canadien William Ehrcke lui répond par un tacle appuyé : « Cette déduction est totalement spéculative et n'a aucun fondement sérieux. Les résidents d'autres pays que les États-Unis, y compris Mme Meng, peuvent avoir une myriade de bonnes raisons pour choisir de ne pas voyager aux États-Unis ces deux dernières années[8]. » Nous sommes le 11 décembre, et Meng Wanzhou est déterminée à se battre.

Cela fait dix jours que la directrice financière de Huawei est incarcérée au centre correctionnel Alouette – mais moins d'une

semaine que la nouvelle de son arrestation s'étale dans les journaux du monde entier, après une fuite dans la presse canadienne. Il y a donc foule, ce mardi-là, devant la Cour suprême de Colombie-Britannique et à l'intérieur de la salle d'audience numéro 20, spécialement équipée de vitres blindées entre la cour et le public, en raison des affaires sensibles – notamment les histoires de gangs – qui y sont jugées d'ordinaire[9]. Xiaozhong Liu, son ex-mari, est au premier rang – il est arrivé à Vancouver dès le 2 décembre, avec leur fille de dix ans. Plusieurs cadres de Huawei sont également présents. Tous attendent de savoir si le juge Ehrcke acceptera de libérer sous caution la prisonnière, dont le visage est à présent connu sur toute la planète. Elle et son ex-époux ont proposé de verser 15 millions de dollars canadiens (10 millions d'euros) comme garantie, en gageant notamment leurs deux maisons de Vancouver, d'une valeur de 14 millions[10]. Mais que représentent ces sommes pour une femme aux ressources potentiellement sans limites ? Le silence prudent de Ren Zhengfei et sa confiance affichée dans le système judiciaire canadien ne sont pas des gages recevables. Un an plus tard, l'évasion rocambolesque de Carlos Ghosn prouvera qu'une garantie de plusieurs millions ne suffit pas à garder un grand dirigeant sous clé. Mais pour l'heure, l'ancien patron de Renault n'a pas encore été libéré sous caution au Japon. Et la justice canadienne est sensible aux arguments des avocats de Meng Wanzhou. D'autant qu'au moins quatre Canadiens – aux professions aussi diverses que professeur de yoga, courtier ou agent d'assurances[11] – sont prêts à se porter personnellement caution, à hauteur de 3 millions de dollars canadiens (2 millions d'euros), pour cette ancienne voisine ou amie. Lorsque le juge rend sa décision, des applaudissements éclatent dans la salle. Contre une caution de 10 millions de dollars canadiens (6,5 millions d'euros), Meng Wanzhou est autorisée à quitter les murs

de sa prison. Les conditions sont toutefois strictes[12]. La directrice financière devra respecter un couvre-feu de 11 heures du soir à 6 heures du matin et ne jamais quitter une zone géographique définie d'un trait de marqueur jaune sur une carte de Vancouver, qui évite soigneusement l'aéroport ou le terminal de ferries. Le respect de cette consigne sera assuré par le port, en permanence, d'une balise GPS. Avant de sortir du tribunal, Meng Wanzhou peut enfin abandonner le survêtement vert des détenus qu'elle porte depuis dix jours. Ses proches lui ont apporté des habits. Mais une épaisse sangle noire entoure désormais sa cheville, et maintient en place un gros boîtier de plastique installé par Recovery Science. Le spécialiste des « programmes d'éthylométrie et de surveillance » facture 540 dollars par mois pour pister les prévenus libérés sous caution. En plus de ce mouchard électronique, un chauffeur et deux gorilles de la société de sécurité privée Lions Gate escorteront nuit et jour Meng Wanzhou, qui assurera leur rémunération. Lorsqu'elle se trouvera chez elle, dans la ravissante villa à un étage bordée de lilas qu'elle possède depuis 2009 dans le quartier cossu de Dunbar-Southlands, à proximité des plages et du campus de la prestigieuse University of British Columbia, un des gardes se trouvera devant le porche aux deux colonnes blanches, l'autre dans la rue de derrière, sur laquelle donne le garage. La cage est dorée, mais cela reste une prison.

La piste iranienne

Selon le traité d'extradition entre le Canada et les États-Unis, ceux-ci disposent de soixante jours après l'exécution d'un mandat d'arrêt pour communiquer les détails de l'accusation et les pièces permettant de statuer sur l'extradition. Alors que le temps passe, la

pression monte. Et le 28 janvier 2019, juste avant l'expiration du délai, c'est une impressionnante galerie d'officiels – parmi lesquels le procureur général des États-Unis, le secrétaire au Commerce, la patronne de la sécurité intérieure ou encore le directeur du FBI – qui se succède au pupitre de la salle de presse, à Washington, pour dévoiler non pas un, mais deux actes d'accusation, devant un parterre dense de caméras et de journalistes[13]. Le premier concerne le groupe Huawei et sa filiale américaine et, à la surprise générale, ressert la vieille histoire du vol de Tappy le robot, six ans plus tôt. L'affaire a été jugée, l'amende, payée. Mais « au cours de son enquête, le FBI a obtenu des e-mails révélant qu'en juillet 2013, Huawei a offert des bonus aux employés sur la base de la valeur des informations qu'ils avaient volées[14] », accuse maintenant Washington – ce que le groupe chinois réfute formellement. Quoi qu'il en soit, le dossier sent méchamment le réchauffé. Le deuxième acte d'accusation concerne, lui, Meng Wanzhou – ainsi que le groupe Huawei et ses filiales américaine et iranienne – à qui il est reproché d'avoir camouflé la violation de sanctions américaines contre l'Iran.

Là aussi, l'accusation n'est pourtant pas de première fraîcheur. Déjà en 2012, dans le rapport au vitriol du Congrès, les auteurs déploraient que Huawei ait « refusé de répondre à des questions précises sur ses activités en Iran ou d'autres pays faisant l'objet de sanctions[15] ». Comme l'ensemble du rapport, ce point manquait cruellement de substance. Mais quelques mois plus tard, une enquête de Reuters allait en apporter[16]. Publié le 31 décembre 2012, cet article contient de quoi faire passer un très mauvais réveillon au groupe de Shenzhen. Le journaliste Steve Stecklow a en effet mis la main sur des documents prouvant qu'un partenaire local de Huawei a proposé de vendre, deux ans plus tôt, à MCI, le premier opérateur mobile iranien, du matériel informatique Hewlett-Packard. Certes, il

n'y en avait que pour 1,3 million d'euros et la transaction ne serait jamais arrivée à son terme. Mais le commerce de ces serveurs et logiciels HP était alors strictement prohibé par les États-Unis (et par HP), dans le cadre des sanctions internationales visant à dissuader Téhéran de poursuivre son programme nucléaire. Et le simple fait de proposer ces produits à un client iranien est amplement suffisant pour s'attirer les foudres de Washington.

Plus encore que cette possible violation des sanctions, c'est l'identité de l'auteur qui intéresse pourtant Steve Stecklow. Le partenaire local de Huawei, une société hongkongaise du nom de Skycom, lui paraît extrêmement proche du groupe de Shenzhen. Sur au moins 13 pages de la proposition commerciale incriminée, le logo de Huawei s'affiche et la mention « Huawei confidential » apparaît. Un an après sa première enquête, le journaliste en rajoute une couche[17]. Non seulement les employés de Skycom seraient nombreux à porter un badge Huawei ou à détenir des cartes de visite Huawei, mais les documents administratifs de la société montreraient qu'elle a appartenu en 2007 à une entreprise de Hong Kong, Hua Ying, elle-même détenue par Shenzhen Huawei Investment & Holding Co Ltd, la maison mère de Huawei. Autrement dit, Skycom et Huawei ne feraient qu'un – et le groupe de Shenzhen se servirait de cet écran pour mener ses activités en Iran. Dans son enquête, Reuters ajoute un élément de poids : la secrétaire générale de Hua Ying en 2007, qui siégera ensuite de février 2008 à avril 2009 au conseil d'administration de Skycom, est une dirigeante de Huawei. Elle s'appelle Meng Wanzhou.

Début 2019, quand la brochette de hauts fonctionnaires dévoile son acte d'accusation contre Meng Wanzhou, tout cela est connu depuis plus de six ans. Pire, le document révèle même qu'en juillet 2007 déjà, le FBI a interrogé Ren Zhengfei en personne au

sujet des activités de Huawei en Iran. Le patron aurait répondu que sa société respectait toutes les lois américaines relatives aux exportations et ne traitait directement avec aucune entreprise iranienne. Mais ce qui a changé pour Washington, c'est qu'à la suite des révélations de Reuters, de nombreuses banques se sont inquiétées. Les grandes organisations financières qui utilisent toutes le dollar – première monnaie d'échange internationale – craignent comme la peste les entreprises suspectées de violer les sanctions internationales car, si leurs transactions transitent par leurs systèmes informatiques, elles peuvent à leur tour être visées par la justice américaine. Après que la BNP a écopé de près de 9 milliards de dollars d'amende à ce titre en 2014, les financiers sont plus vigilants que jamais.

La direction de la banque britannique HSBC est également échaudée. En 2012, le groupe a pour sa part dû régler près de 2 milliards de dollars pour mettre fin à une enquête de la justice américaine sur des mauvaises pratiques anti-blanchiment et des transactions violant certaines sanctions américaines[18]. Dans le cadre de son accord avec les autorités, HSBC s'est également engagée à coopérer avec les futures investigations du Département de la justice. Et, toujours selon l'agence Reuters, c'est précisément ce qui s'est passé concernant Huawei[19]. Après avoir mené une enquête interne sur Skycom en 2016 et 2017, HSBC aurait conclu que le groupe de Shenzhen avait maintenu des liens financiers très étroits avec son soi-disant partenaire. Ainsi, la coquille juridique qui a hérité des actions de Skycom après Hua Ying, une entreprise enregistrée à l'île Maurice sous le nom de Canicula Holdings, aurait été contrôlée et financée par Huawei en sous-main. Conformément à son engagement de délinquante repentie, la banque aurait ensuite présenté l'ensemble de ces conclusions à la justice américaine.

Grâce à ces éléments, celle-ci pense pouvoir coincer Meng Wanzhou. La directrice financière n'est impliquée directement dans aucune des transactions iraniennes de Skycom, mais c'est par son entremise que HSBC aurait accepté de continuer à traiter les opérations du groupe chinois et de Skycom. En camouflant sciemment les liens de Huawei avec ce que les États-Unis appellent désormais « sa filiale iranienne Skycom », la dirigeante aurait fait courir d'importants risques financiers à HSBC et d'autres – ce qui serait constitutif, selon l'acte d'accusation, de fraude bancaire et de fraude électronique. Concrètement, Meng Wanzhou aurait fait une présentation mensongère à un cadre de HSBC, au cours d'une réunion tenue le 22 août 2013, dans l'arrière-salle d'un restaurant de Hong Kong. HSBC avait elle-même demandé des clarifications sur la nature des activités de Huawei en Iran. Quoique parfaitement à l'aise en anglais, Meng parlait en mandarin et était accompagnée d'un traducteur – sans doute pour éviter toute approximation sur un sujet hautement sensible. La jeune quadragénaire s'appuyait sur une présentation PowerPoint reprenant les points clés de son argumentaire, notamment l'idée que Huawei « opère en Iran dans le strict respect des lois, régulations et sanctions des Nations unies, des États-Unis et de l'Union européenne en vigueur » et que sa présence au conseil d'administration de Skycom n'avait pour but que de « renforcer et veiller sur la conformité de Skycom »[20]. Autant d'inexactitudes, selon Washington, convaincu que Skycom n'est qu'une façade derrière laquelle s'est abrité le géant chinois pour contourner les sanctions et fournir à l'Iran du matériel prohibé, « y compris des équipements de surveillance utilisés pour suivre, identifier et détenir des manifestants durant les manifestations anti-gouvernementales de 2009 à Téhéran ». Selon l'acte d'accusation, des transactions d'une valeur totale de plus de 100 millions de dollars

liées à Skycom ont transité par les États-Unis. Et la personne qui a camouflé ce risque majeur à HSBC et d'autres organismes financiers se trouverait maintenant à Vancouver, devant la Cour suprême de Colombie-Britannique – qui dispose notamment d'une copie du PowerPoint pour décider de son extradition vers les États-Unis.

ZTE, le coup de semonce

En dépit du choc de l'arrestation de Meng Wanzhou, Huawei pouvait se douter que les nuages qui s'amoncelaient depuis des années au-dessus de ses activités iraniennes finiraient par déclencher un violent orage – pour la simple raison qu'un autre groupe de télécoms chinois avait suivi un peu plus tôt une trajectoire étonnamment similaire. Si ce n'est par la taille – il ne pointe qu'en quatrième position des équipementiers télécoms mondiaux –, ZTE ressemble en bien des points à son grand rival domestique Huawei. Les deux groupes sont voisins, à Shenzhen, depuis leur création au mitan des années 1980, et tous les deux ont fait fortune en équipant les réseaux fixes puis mobiles de la Chine et des pays émergents. En dépit d'un appui officiel de l'État chinois, puis d'une introduction en Bourse pour se donner les moyens d'accélérer son développement, ZTE n'a pas rencontré un succès aussi extraordinaire que Huawei, particulièrement chez les grands opérateurs occidentaux. En revanche, il s'est attiré les mêmes suspicions des États-Unis. Le rapport du Congrès américain de 2012 qui barrera *de facto* le chemin aux équipementiers chinois faisait, quasiment à l'identique, les mêmes reproches aux deux entreprises.

Le parallèle est encore plus frappant en ce qui concerne les relations à l'Iran. Quelques mois avant de publier son enquête sur

Huawei et Skycom, le même journaliste de Reuters, Steve Stecklow, avait en effet révélé que ZTE avait livré à l'Iran un puissant système de surveillance des communications électroniques[21], puis que le groupe chinois avait accepté de fournir à un grand opérateur télécoms iranien des millions de dollars d'équipements informatiques de constructeurs américains – IBM, Cisco, Oracle, Symantec… –, au mépris des sanctions en vigueur. Comme pour Huawei, ces révélations dans la presse pousseront la justice américaine à mettre son nez dans le dossier. L'enquête durera cinq ans, avant que, le 7 mars 2017, le secrétaire au Commerce Wilbur Ross annonce la plus forte sanction civile et pénale jamais prononcée contre un groupe industriel pour avoir enfreint un embargo américain[22]. Non seulement ZTE s'est joué des sanctions en vigueur, mais des équipes internes étaient chargées d'effacer toutes les traces des transactions illégales. Le groupe chinois a reconnu sa culpabilité dans l'export de centaines de millions de dollars de marchandises, dont des routeurs, serveurs et microprocesseurs américains, en direction de l'Iran, mais aussi de la Corée du Nord – et doit verser 1,2 milliard de dollars au Trésor américain. En plus de cette copieuse amende, ZTE s'est engagé à mettre en place un strict système d'audit pour empêcher toute récidive. S'il ne remplissait pas les termes de l'accord, l'administration américaine a prévenu qu'elle n'hésiterait pas à le couper de tous ses fournisseurs américains. « Ceux qui enfreignent nos sanctions économiques, lois de contrôle des exportations et tout autre régime commercial ne resteront pas impunis – ils subiront les conséquences les plus pénibles », gronde Wilbur Ross à la tribune, ajoutant que « cette affaire n'est que le début »[23].

Huawei avait dès lors de quoi se faire des cheveux blancs. D'autant qu'un des documents internes à ZTE et rendu public par le BIS est porteur d'une lourde menace[24]. Dans ces neuf pages, toutes

marquées « Secret – Highly confidential », ZTE détaille les risques et mesures de protection liés à ses opérations dans cinq pays sous embargo : l'Iran, le Soudan, la Corée du Nord, la Syrie et Cuba. Le groupe déplore que l'« entreprise tampon » à laquelle il a recours en Iran ne soit pas suffisamment bien dotée en capital et en capacités pour jouer efficacement son rôle de pare-feu et vante la méthode bien plus performante d'une autre entreprise, désignée sous le nom de code « F7 ». L'identifier ne prend pas bien longtemps. ZTE écrit un peu plus bas qu'« en 2010, la proposition de F7 d'acquérir l'entreprise américaine 3Leaf s'est heurtée à l'opposition du gouvernement américain, citant l'impact sur la sécurité nationale », une description qui ne peut coller qu'à son grand frère de Shenzhen, Huawei.

Malgré cette première volée de bois vert, ZTE était loin d'en avoir fini avec l'administration américaine. Un an après sa première sortie contre ZTE, le secrétaire au Commerce Wilbur Ross vilipende à nouveau le groupe chinois, accusé de n'avoir pas tenu ses engagements[25]. Les dirigeants de ZTE auraient tort de se fier au débit lent et au visage impassible de l'octogénaire, qui lui donnent un air de vénérable tortue. L'ex-banquier d'affaires ne fait pas dans les sentiments. Wilbur Ross a fait fortune en redressant des entreprises à coups de serpe, gagnant au passage le surnom de « roi des faillites ». Un syndicaliste américain a dit de lui un jour qu'il était « un peu comme le chirurgien qui peut vous garder en vie, mais en vous coupant la jambe[26] ». Et ce jeudi 7 juin 2018, le secrétaire américain est prêt à trancher dans le vif. Car ZTE aurait menti aux autorités américaines. Au lieu de sanctionner les dirigeants impliqués dans ses transactions illégales, le groupe leur aurait carrément attribué des bonus. Cette fois, Washington voit rouge. Le Département du commerce met sa menace à exécution et demande au BIS de placer immédiatement ZTE sur son « Entity List » – une liste noire des

organisations étrangères avec lesquelles les entreprises américaines ont l'interdiction absolue de commercer, à moins d'obtenir une licence spéciale d'exportation. ZTE avait été prévenu, mais le coup n'en est pas moins terrible. Privée soudainement de tout approvisionnement en produits américains, qui constituent 25 à 30 % des composants utilisés dans ses antennes comme dans ses téléphones[27], la société est notamment coupée de son fournisseur de processeurs mobiles Qualcomm, mais aussi des applications mobiles de Google. Dans une lettre à ses 75 000 salariés, le patron de ZTE Yin Yimin explique que le groupe se trouve dans « une situation internationale compliquée ». C'est un bel euphémisme. Les échanges sur les actions ZTE sont suspendus à la Bourse de Hong Kong et de Shenzhen (ils ne reprendront que plusieurs semaines plus tard, et le cours enregistrera une chute de quasiment 60 % à la suite de la crise). Le 9 mai, ZTE informe ses actionnaires que « les principales activités opérationnelles de l'entreprise ont cessé[28] ». Les usines arrêtent de tourner, faute de composants. Les boutiques ne sont plus approvisionnées en smartphones de la marque, qui disparaissent aussi des grandes plateformes chinoises d'e-commerce[29]. Le quatrième équipementier mondial, qui est aussi un acteur non négligeable du marché des smartphones, pourrait bien, en l'espace de quelques semaines, mettre la clé sous la porte. Son salut viendra, curieusement, de Donald Trump. Le 13 mai, le président américain tweete : « Le président chinois Xi et moi travaillons ensemble à donner à la géante entreprise de téléphone chinoise ZTE un moyen de reprendre son activité, vite. Trop d'emplois perdus en Chine. Le Département du commerce a reçu l'instruction de le faire[30] ! » Quelques semaines plus tard, Wilbur Ross annonce un nouvel accord avec ZTE[31]. Le nom du groupe chinois est retiré de l'infamante « Entity List », mais il doit renouveler entièrement son équipe

dirigeante, ainsi que son conseil d'administration dans les trente jours. Et s'acquitter d'un nouveau milliard de dollars d'amende. La balle n'est pas passée loin. Et les séquelles se feront sentir encore longtemps, tant les clients de ZTE ont été effrayés par la perspective d'être soudain privés de tout support ou nouveaux équipements. L'opérateur italien Wind-Tre, un des rares opérateurs en Europe de l'Ouest qui avait signé un mirobolant contrat de près d'un milliard d'euros avec ZTE fin 2016, ne tardera pas à changer de cheval. À l'été 2018, il fera affaire avec le suédois Ericsson pour changer ses antennes, moyennant 600 millions d'euros. Mais le plus important, c'est que les États-Unis ont fait l'éclatante démonstration de leur puissance. En utilisant l'arme des embargos, ils peuvent étrangler à mort une grande entreprise technologique étrangère. ZTE n'a été que la répétition générale. Huawei va bientôt suffoquer à son tour.

Le piège américain

Si une personne au monde a été particulièrement attentive à tous les épisodes du feuilleton ZTE, c'est Meng Wanzhou. Fin 2018, alors que la directrice financière de Huawei se retrouve prisonnière au Canada, ZTE a pu reprendre, tant bien que mal, son activité depuis quelques mois. Mais certaines réflexions de Donald Trump continuent de résonner, comme ce tweet présidentiel du 14 mai 2018 expliquant que ZTE « achète un grand nombre de pièces à des entreprises américaines » et que cela « reflète aussi l'accord commercial plus large que nous négocions avec la Chine »[32] ou cet autre, du 26 mai, se rengorgeant d'avoir fermé et laissé rouvrir l'entreprise en échange d'une obligation « à acheter des pièces américaines[33] » – avant de préciser que « les Dems ne font rien… », dans un élan très trumpien.

La question qui se pose est simple. La Maison-Blanche a-t-elle utilisé les pressions judiciaires sur ZTE pour pousser son agenda politique ? La survie du deuxième équipementier chinois a-t-elle servi de monnaie d'échange dans le bras de fer commercial avec Pékin ? Après tout, et après des mois d'escalade, la Chine a fini par consentir à des achats massifs de produits américains fin 2018, afin de redresser un peu sa balance commerciale structurellement excédentaire avec Washington. L'accord a été scellé le jour même de l'arrestation de Meng Wanzhou à l'aéroport de Vancouver.

Pour les avocats de la dirigeante de Huawei, la même question mérite d'être posée concernant leur cliente : derrière leurs accusations tarabiscotées de fraude bancaire, les Américains ont-ils en réalité voulu prendre un otage dans leur guerre commerciale avec Pékin ? Ou dans leur guerre technologique à l'approche de la 5G ? Bien sûr, le jour où les charges ont été dévoilées à Washington, Wilbur Ross s'en est défendu : « Pour être clair, ces actes d'accusation sont des mesures d'application de la loi et sont entièrement distincts de nos négociations commerciales avec la Chine[34]. » Mais si le secrétaire au Commerce a pris la peine de réfuter, c'est que bien des observateurs se font la réflexion. Parmi eux, les avocats de Meng Wanzhou n'ont d'ailleurs pas hésité à pousser cet argument auprès de la Cour suprême de Colombie-Britannique, en s'appuyant sur les déclarations de Donald Trump lui-même. Le bouillonnant 45e président des États-Unis, peu connu pour son profond respect des procédures judiciaires, a en effet déclaré à l'agence Reuters, le 12 décembre 2018, être tout à fait prêt à intervenir dans l'affaire Meng Wanzhou si cela faisait avancer son « deal » avec la Chine – « qui sera certainement le plus vaste accord commercial jamais conclu – ce qui est une chose très importante –, ce qui est bon pour la sécurité nationale[35] », justifie-t-il.

Quoi qu'en dise la justice américaine, il est difficile de ne pas sentir le poids de la politique internationale dans l'imbroglio canadien. Le jour même où l'arrestation de Meng Wanzhou était rendue publique, l'ambassade de Chine au Canada a protesté vigoureusement contre de « sérieuses violations des droits humains de la victime[36] » et demandé la libération immédiate de sa ressortissante. Parfois, la politique s'invite dans de tout petits détails, comme lors de l'audience à l'issue de laquelle la fille de Ren Zhengfei sera remise en liberté (très surveillée). À deux reprises ce jour-là, une sonnerie de portable inhabituelle résonne dans la salle du tribunal de Vancouver[37]. Tout en cuivres et en roulements de tambour, il s'agit de *La Marche des volontaires*, l'hymne national de la République populaire de Chine. L'incident est rapidement clos par une discrète sortie de l'indélicat propriétaire de ce bruyant téléphone. Mais c'est un signe anodin, parmi d'autres, de l'affrontement des puissances qui se joue en réalité derrière le box de l'accusée. Quelques heures plus tard, quand Meng ressort libre, sous caution, elle prend le temps de poster une seule image sur la messagerie WeChat, qui devient rapidement virale en Chine. C'est une ancienne publicité de Huawei, où l'on voit les deux pieds d'une ballerine – l'un encore dans son chausson nacré ; l'autre, nu et meurtri par les entraînements – accompagnés du slogan : « Derrière la grandeur, il y a la souffrance. » Meng Wanzhou a ajouté quelques mots : « Je suis à Vancouver, aux côtés de ma famille. Je suis fière de Huawei, et fière de mon pays. Merci à tous ceux qui m'ont manifesté de l'attention. »

Celle que l'opinion publique chinoise considère comme une otage économique, technologique et politique a ouvert une porte de sa cage. Il reste à ses avocats à faire capoter la demande d'extradition pour qu'elle puisse s'envoler. Pour cela, les cadors du barreau qui l'assistent ont un raisonnement béton : Meng Wanzhou n'aurait

jamais été condamnée au Canada pour des faits similaires à ceux qui lui sont imputés par les États-Unis, car il n'y existe pas de restrictions aux exportations en direction de l'Iran. Or, pour qu'un détenu soit extradé aux États-Unis, il faut que cette condition de « double criminalité » soit remplie, c'est-à-dire que l'infraction supposée soit répréhensible légalement au Canada. Près de deux ans après l'arrestation de la dirigeante, ses équipes légales sont persuadées de tenir là son billet vers la liberté. L'« otage » va-t-elle s'échapper ? Samedi 23 mai 2020, quatre jours avant le verdict, des journalistes de la chaîne télévisée canadienne CBC surprennent en tout cas une étrange scène sur les marches de la Cour suprême de Colombie-Britannique, en plein cœur de Vancouver[38]. Un shooting photo est en train de s'y mettre en place, quand surgit une grosse automobile, dont s'extrait Meng Wanzhou, dans une robe noire sans manches. En quatre minutes chrono, elle s'est positionnée au milieu d'une dizaine de ses proches, a posé pour le photographe, sourire aux lèvres et pouce levé en signe de victoire, puis est remontée dans son véhicule. Les images devaient-elles servir à illustrer la liesse de la victoire judiciaire ? Si tel est le cas, elles n'ont pas eu d'emploi. Le mercredi suivant, la juge Heather Holmes rend sa décision et estime que la condition de « double criminalité » est bien remplie. La magistrate a considéré que l'accusation ne portait pas sur une violation des sanctions américaines mais sur la fraude bancaire qui, elle, est condamnable en droit canadien. Les espoirs de la défense retombent comme un soufflé. Mais il leur reste bien des cartes à jouer pour éviter que leur cliente ne soit emmenée aux États-Unis, où elle risque des dizaines d'années de prison. Les avocats ont déjà dénoncé la collusion entre le FBI, la police montée et les douanes, qui ont interrogé Meng Wanzhou pendant trois heures sans avocat à sa descente d'avion. Ils ont aussi demandé l'intervention du

gouvernement canadien qui, bien qu'il s'en défende, a toujours son mot à dire en dernier ressort dans les affaires d'extradition – qu'il peut parfaitement décider de stopper à tout moment dans le cadre de sa politique étrangère. Surtout, la défense de Meng Wanzhou compte bien relever la dimension commerciale que Donald Trump lui-même a donnée à l'affaire, pour dénoncer la duplicité des autorités américaines. Washington ne mène-t-il pas un combat bassement économique avec des armes juridiques ?

Cette thèse est en tout cas celle d'un Français, dont le livre fait fureur en Chine depuis qu'un journaliste de Bloomberg a publié une photo du bureau de Ren Zhengfei – un an jour pour jour avant l'énoncé du verdict de la juge Holmes[39]. Devant le grand tableau d'un paysage alpin et une bibliothèque emplie de livres, documents et photos, la table de travail du patron est également recouverte d'un joli fatras, mais, bien en évidence, un épais volume gris se détache, avec son titre en gros caractères blancs. Il s'agit de la traduction chinoise de l'ouvrage publié en janvier sous le titre *Le Piège américain*[40]. Frédéric Pierucci, ex-patron d'une des filiales du géant de l'énergie et des transports français Alstom, y raconte par le menu comment les États-Unis l'ont pris en otage pour faire pression sur son entreprise. Cinq ans avant Meng Wanzhou, lui aussi voyage sur un Boeing 777 de la Cathay Pacific, mais, malheureusement pour lui, à destination de New York. À son arrivée à l'aéroport JFK, le cadre français est aussitôt arrêté, menotté, emmené au siège du FBI et inculpé pour une affaire de corruption impliquant Alstom en Indonésie dont il assure pourtant n'avoir jamais touché un seul centime. Affublé de la tenue orange des prisonniers américains, il passera deux ans derrière les verrous, sous le matricule 26613, dont quatorze mois dans la puanteur et les cris de la prison de haute sécurité de Wyatt, Rhode Island. Alstom, son employeur, l'abandonne

à son sort pour négocier avec la justice américaine un renoncement aux poursuites pour corruption moyennant une amende record de 772 millions de dollars… L'accord est finalement conclu trois jours après que le groupe français a accepté de céder sa filiale énergétique – y compris l'activité stratégique de fabrication de turbines pour les centrales nucléaires françaises – à l'Américain General Electrics pour 12 milliards d'euros. Pour Frédéric Pierucci, la manœuvre est très claire. Les États-Unis utilisent sans vergogne leurs lois extraterritoriales, comme le Foreign Corrupt Practices Act sanctionnant la corruption à l'étranger, pour cibler des entreprises stratégiques et les affaiblir ou, dans le cas d'Alstom Energie, les racheter. Le paravent légal de la lutte anti-corruption, que la justice américaine mène de manière très sélective, cache mal une entreprise de déstabilisation économique.

Il n'est pas surprenant que l'ouvrage français ait fait un tabac à Shenzhen. Non seulement il trône sur le bureau de Ren Zhengfei, mais le groupe en fait la promotion sur son campus. Ainsi, sur le pharaonique site de Dongguan – avec ses répliques des grands monuments européens –, le quartier français comporte une version, assez kitsch, du café de Flore, où les passants ne peuvent rater la grande affiche du *Piège américain*, décrit comme « un incident en France semblable à celui de Huawei[41] ». En mars 2019, Ren Zhengfei s'autorise une sortie face aux journalistes du *LA Times* : « N'est-ce pas vrai que dans le passé le gouvernement américain s'est attaqué à Alstom et à Toshiba ? Vu de ce côté-là, le gouvernement américain n'a pas une très belle réputation. Il est donc normal que le gouvernement chinois laisse entendre sa voix de colère. » En privé, les équipes de Huawei n'hésitent pas non plus à faire le rapprochement avec le sort réservé par Washington à son grand concurrent suédois Ericsson, lui-même condamné à une mirifique amende de plus d'un milliard de

dollars en décembre 2019 pour avoir enfreint le Foreign Corrupt Practices Act en Chine et dans d'autres pays. La justice américaine ne fait-elle que sanctionner des actes répréhensibles – même si l'on pourrait arguer qu'ils ne se sont pas produits sur son sol ? Ou cible-t-elle spécifiquement, dans l'océan de la corruption mondiale, quelques entreprises – comme les champions chinois et européens de la 5G – pour affaiblir l'un et obtenir des leviers sur l'autre ? Huawei est parfaitement légitime à poser la question au printemps 2019. Mais cela ne sauvera pas le groupe du drame. Après avoir englouti Meng Wanzhou, le piège américain va maintenant se refermer sur le numéro 1 mondial des télécoms.

La liste noire

Dans la dernière ligne droite vers la 5G, deux dates sont incontournables pour comprendre comment la fracture technologique entre la Chine et les États-Unis va soudainement s'ouvrir. La première est le 1er décembre 2018, quand Meng Wanzhou – pour des motifs apparemment sans aucun lien avec les télécommunications – est arrêtée et devient à son corps défendant l'incarnation de la bataille des deux superpuissances du XXIe siècle. La seconde est le 16 mai 2019, lorsque les États-Unis placent Huawei, le champion chinois de la 5G, sur leur « Entity List » – le registre des entreprises parias sur lequel ils avaient brièvement inscrit ZTE un an plus tôt. Nous allons y revenir, mais pas sans souligner que ces deux crises aiguës ne surgissent pas du néant. Elles sont l'aboutissement d'une défiance de vingt ans, qui ne fait que s'accélérer sur les deux dernières années.

En janvier 2018, c'est d'abord l'opérateur AT&T qui est contraint par l'administration américaine d'annuler son accord de distribution

des derniers téléphones haut de gamme de Huawei. L'annonce devait en être faite par Richard Yu, le patron de la branche Smartphones du groupe chinois, sur la scène du Consumer Electronic Show (CES) de Las Vegas, le grand événement tech de la planète. Mais à quelques jours du salon, tout tombe à l'eau. Le dirigeant chinois ne pourra profiter de la tribune que pour regretter une « grande perte pour Huawei », mais une perte encore plus importante pour les consommateurs américains, privés des smartphones Huawei. Quelques semaines plus tard, c'est au tour de Verizon, le numéro 2 du mobile aux États-Unis, de se défausser. Puis, début février, nouveau coup dur. Les six responsables des plus grandes agences de renseignement américaines – dont les patrons du FBI, de la NSA et de la CIA – sont auditionnés au Sénat. Et tous restent impeccablement silencieux et immobiles quand il leur est demandé : « Levez la main si vous recommanderiez à des citoyens américains d'utiliser des produits ou services de Huawei ou ZTE[42]. » Il flotte un parfum funèbre. Encore trois mois et la vente des smartphones Huawei est interdite sur les bases militaires américaines ; six mois et ce sont les agences fédérales qui ont interdiction de s'approvisionner chez les deux géants des télécoms de Shenzhen…

Une secousse tellurique massive va faire oublier tous ces tremblements mineurs. Elle survient le 16 mai 2019. En plaçant Huawei et 68 de ses filiales internationales sur sa liste noire, le BIS inflige ce jour-là un coup comme jamais le groupe de Shenzhen, ni aucun acteur technologique de cette taille, n'en a encore reçu. La règle édictée est simple : si un produit contient plus de 25 % de composants américains ou s'il est fabriqué à partir de technologies américaines, il est interdit de le vendre à Huawei – à moins d'obtenir une autorisation en bonne et due forme du Département du commerce. L'onde de choc peut se répercuter dans toute la chaîne

d'approvisionnement. Huawei est un énorme client pour nombre d'industriels aux États-Unis. « Nous sommes le troisième plus grand acheteur des puces américaines du monde. S'ils ne nous vendent pas leurs puces, beaucoup d'entreprises américaines verront chuter leurs ventes, ce qui par la suite impactera leur performance sur le marché boursier[43] », avait anticipé Ren Zhengfei deux mois plus tôt.

Face à ce probable retour de bâton, les États-Unis tentent d'amortir le choc et annoncent, le lundi suivant leur coup de massue, une licence générale temporaire de 90 jours. L'interdiction ne doit prendre effet qu'au 19 août, pour laisser le temps aux fournisseurs de Huawei de se retourner. De trois mois en trois mois, cette licence générale sera repoussée continuellement jusqu'à l'été 2020. Mais l'épée de Damoclès n'est que suspendue. Et Donald Trump s'amuse à jouer avec cette arme dans ses négociations commerciales. À l'été 2019, au cours d'une nouvelle réunion du G20, il déclare autoriser les entreprises américaines à vendre au groupe chinois des équipements « pour lesquels il n'y a pas de gros problème d'urgence nationale », avant d'ajouter que « Huawei est une situation compliquée. Nous avons convenu de laisser cela – nous laissons Huawei pour la fin. Nous allons voir. Nous verrons où nous allons avec l'accord commercial ». Mais le président maîtrise-t-il encore le monstre qu'il a libéré ? Dans la foulée de ses déclarations du G20, des députés déposent une proposition de loi bipartisane – autant dire un ovni en ces temps de division politique exacerbée aux États-Unis – visant à empêcher le président de lever l'embargo sur Huawei sans l'accord préalable du Congrès : le Defending America's 5G Future Act. Entre républicains et démocrates, on s'accorde sur peu de choses, si ce n'est l'impérieuse nécessité de barrer la route au champion chinois de la 5G.

Le premier effet manifeste du placement sur la liste noire est l'annonce brutale par Google qu'il cessera de fournir à Huawei son système d'exploitation mobile Android – le logiciel qui fait tourner neuf téléphones sur dix dans le monde et l'intégralité des appareils Huawei. Seuls les modèles disponibles au public avant le 16 mai 2019 continueront de bénéficier des mises à jour du géant de Mountain View. Plus encore que les puces américaines – pour lesquelles Huawei compte alors sur les alternatives internationales comme celles du Taïwanais Mediatek ou tout simplement sa propre production, qui n'a rien à envier aux semi-conducteurs américains grâce aux prouesses de sa filiale HiSilicon –, la soudaine disparition des services de Google pose un sérieux problème au groupe chinois. Le socle d'Android est dit open source, c'est-à-dire que Google a mis le code à disposition de tous et qu'une grande variété de contributeurs – dont Huawei – participent à son évolution. Les nouveaux appareils de Huawei pourront certes utiliser cette version de base, voire – ses ingénieurs y travaillent depuis des années, on ne va pas tarder à l'apprendre – utiliser un nouveau système d'exploitation construit à partir de cette brique fondamentale. Mais les services que Google fournit avec sa version propriétaire d'Android sont difficilement remplaçables. Il y a d'abord le magasin d'applications Google Play – qui recense les millions d'applis mobiles validées par Google. D'autres magasins existent, mais la sécurité est rarement au rendez-vous et le risque pour les consommateurs de télécharger une appli malveillante est réel. Il y a surtout les propres applications développées par Google : Maps, Gmail, Agenda, Docs, Drive… Pour le marché chinois, ce n'est pas un problème. Google en est absent de longue date et d'autres applis remplissent les mêmes fonctions. Mais en Europe, le deuxième marché du constructeur pour ses smartphones, c'est presque un arrêt de mort. Vendre un téléphone

Android sans les services de Google est une gageure. Les sanctions américaines sont encore plus efficaces sur la demande des consommateurs que sur l'offre de Huawei – encore capable de produire ses téléphones et ses antennes, quoique dans des conditions difficiles.

L'option nucléaire

Huawei est sonné, mais le pire reste à venir. S'insérant dans les interstices de l'interdiction américaine, le groupe chinois continue à se fournir en puces étrangères. Il a même gonflé ses commandes au maximum des capacités de ses fournisseurs pour faire des stocks, au cas où. Il fait bien. Le 17 août 2020, Wilbur Ross annonce une salve de nouvelles mesures[44]. Le secrétaire au Commerce est résolu à boucher les trous et à étouffer Huawei. Pour cela, il décrète que l'interdiction de commercer avec Huawei et ses filiales est étendue. Elle concerne désormais tous les éléments produits à l'étranger en utilisant « des technologies ou logiciels américains ». C'est extrêmement large. Et cela vise – le secrétaire au Commerce n'en fait pas mystère – l'approvisionnement de Huawei en puces électroniques, qui sont toutes fabriquées avec « des technologies ou logiciels américains » à un moment ou à un autre.

La propre filiale de Huawei, HiSilicon, ne fait que concevoir des puces extrêmement performantes. Pour les fabriquer, elle s'appuie sur les usines géantes de TSMC. La Taïwan Semiconductor Manufacturing Company, malgré ses 30 milliards d'euros de revenus annuels, est peu connue du grand public. Pourtant, ce sont de ses lignes de production – majoritairement situées sur l'île de Taïwan – que sortent plus de la moitié des puces utilisées dans le monde et

notamment les plus haut de gamme. Apple, Qualcomm, Nvidia ou Huawei, tous ont recours aux services de TSMC. C'est le seul acteur, avec le Sud-Coréen Samsung, à maîtriser les processus de gravure de transistors sur les plaques de silicium à une échelle de 7 nanomètres, et bientôt 5. Cela revient à créer 10 000 minuscules interrupteurs sur l'épaisseur d'un cheveu. Même le géant américain Intel a abandonné cette course à l'infiniment petit, trop gourmande en capital. Mais pour réaliser cette prouesse technologique, TSMC utilise de nombreuses machines et technologies… américaines. Wilbur Ross a été très clair. Si le Taïwanais ne veut pas tomber dans le collimateur des États-Unis – qui restent son premier client –, il doit cesser de fournir Huawei.

Pour le groupe chinois, c'est une catastrophe, car il n'y a tout simplement pas d'alternative crédible à TSMC. La seule fonderie chinoise qui joue dans la cour des grands pointe à la cinquième place mondiale. Elle s'appelle SMIC (Semiconductor Manufacturing International Corporation) et a des années de retard technologique sur TSMC. HiSilicon peut se rabattre sur ses usines, mais certainement pas pour fabriquer des processeurs aussi puissants que les Kirin qui équipent ses meilleurs smartphones. « Cette année pourrait marquer la fin des puces haut de gamme Kirin de Huawei, la dernière génération[45] », reconnaît en août 2020 Richard Yu, le patron de la branche Smartphones.

Privé des puces américaines et des fournisseurs de tierce nationalité comme Mediatek, Sony ou le français STMicro, qui dépendent tous des technologies américaines pour concevoir et produire leurs composants, Huawei n'a même plus la possibilité de faire fabriquer ses propres processeurs. Sans ces éléments indispensables, comment produire téléphones et antennes ? Ou même assurer le service après-vente des équipements installés ? Pour

de nombreux observateurs, les annonces de Wilbur Ross sont une condamnation à mort. L'éditorialiste de Bloomberg, Tim Culpan, fin connaisseur de l'industrie du semi-conducteur et particulièrement de TSMC, écrit le 18 août : « Trump vient de choisir l'option nucléaire contre Huawei. Les choses pourraient très vite mal tourner[46]. » En ce qui concerne les relations internationales, c'est inévitable. Et pour ce qui est du champion chinois, elles ont déjà tourné au vinaigre. En deux ans de pilonnage incessant, les États-Unis l'ont considérablement affaibli et, ce qui est plus grave, ont progressivement détourné de la 5G chinoise un nombre croissant de pays.

CHAPITRE VII

Les dominos

Comment contenter les États-Unis, un allié stratégique, sans froisser la Chine, un partenaire économique incontournable ? La question fait s'arracher les cheveux à bien des gouvernements. Washington ne cache plus son intransigeance sur le sujet des équipements télécoms chinois. Une capitale après l'autre, les positions se dessinent. Et la crise devient mondiale.

Five Eyes

James Bond sait vivre. L'agent 007 ne refuserait certainement pas un agréable dîner, en bord de mer, avec du homard au menu, arrosé de quelques bouteilles de vin de la Nouvelle-Écosse. Le soir du 17 juillet 2018, c'est l'alléchant programme qui réunit à Halifax, sur la façade atlantique du Canada, un petit groupe de maîtres espions anglo-saxons – ce qu'on fait de plus ressemblant dans la réalité au héros des romans de Ian Fleming. Ces agapes, qui ne seront dévoilées que plusieurs mois plus tard par la presse australienne[1], viennent clore les deux jours de réunion annuelle des Five Eyes, qui se tenaient

cette année-là à Ottawa. Derrière cette appellation « Cinq Yeux » se cache la plus puissante association de services de renseignements du monde. Une alliance dont les origines remontent à la Seconde Guerre mondiale et qui réunit les services secrets des États-Unis, du Royaume-Uni, du Canada, de l'Australie et de la Nouvelle-Zélande. En cette agréable soirée de juillet, le Premier ministre canadien Justin Trudeau est venu partager un verre avec les hommes de l'ombre. Les sujets de conversation ne manquent pas, mais deux thèmes dominent. Le premier est l'enquête sur l'assassinat de Sergueï Skripal, un ex-agent double russe, en plein cœur de l'Angleterre, au printemps précédent. Son empoisonnement à l'aide d'un agent neurotoxique appelé Novitchok pointe si évidemment vers Moscou qu'il a déclenché dans tous les pays occidentaux la plus importante vague d'expulsions de diplomates et d'agents de renseignement russes depuis la fin de la guerre froide. Le second sujet qui préoccupe les espions est la montée en puissance de la Chine et de Huawei.

Les États-Unis ne peuvent qu'inciter leurs plus proches alliés à durcir le ton face à Pékin et à brider les ambitions de son champion de la 5G. À Halifax, c'est la nouvelle patronne de la CIA qui se charge de porter le message. Première femme à diriger la célèbre agence de renseignement américaine, Gina Haspel a le physique anodin des parfaits agents de l'ombre : stature moyenne, cheveux châtains ondulant autour d'un visage rond, yeux marron, lèvres minces et pommettes légèrement saillantes. Avec ses sages lunettes, on pourrait la croire institutrice, médecin ou, pourquoi pas, comptable. On aurait tort de s'y fier. Gina Haspel n'est pas une tendre. L'espionne de carrière déclarait deux mois plus tôt lors de son audition par le Sénat avoir toujours excellé à récupérer des informations secrètes lors de « rendez-vous dans des ruelles poussiéreuses des capitales du tiers-monde ». C'est surtout son passage à la tête d'une prison secrète en

Thaïlande qui a fait tiquer certains élus et couler beaucoup d'encre. La CIA y aurait eu recours à la torture, notamment à la très controversée méthode du « waterboarding[*1] » pour interroger des membres d'Al-Qaeda. Gina Haspel aurait ensuite participé à la destruction des vidéos[2]. Nul doute que cette professionnelle sait mettre le ton pour convaincre ses homologues des Five Eyes de contrer la Chine et Huawei, même s'ils ont historiquement des positions très différentes face à l'équipementier chinois. Le Royaume-Uni, notamment, lui a ouvert largement ses portes depuis plus de dix ans.

Les plus réceptifs aux pressions américaines sont probablement les espions australiens. Un mois après le dîner d'Halifax, le Premier ministre australien Michael Turnbull prend son téléphone pour appeler Donald Trump. Sa décision est prise, il en a réservé la primeur au président américain. Quatre jours plus tard, il la rend publique. Le 23 août 2018, faisant valoir un impératif de sécurité nationale, l'Australie devient le premier pays à exclure officiellement Huawei et ZTE de ses futurs réseaux 5G. Même les États-Unis ne font alors que « recommander » à leurs opérateurs de ne pas utiliser le matériel chinois. Après quinze ans de présence et des investissements conséquents en Australie, la branche locale de Huawei déplore sur Twitter « un résultat très décevant pour les consommateurs », tandis que le ministère chinois des Affaires étrangères dénonce des « excuses pour artificiellement ériger des barrières et recourir à des pratiques discriminatoires », et presse le gouvernement australien « d'abandonner les préjugés idéologiques et de fournir un environnement concurrentiel équitable aux entreprises chinoises »[3].

Des espions au pupitre

Ce 23 août 2018, l'Australie est le premier domino que Washington réussit à faire tomber. C'est aussi le plus facile. Depuis des années, Canberra se méfie des ambitions technologiques de son grand voisin asiatique. Déjà en 2012, le même Michael Turnbull – alors ministre des Communications – avait empêché, sur recommandation des services de sécurité australiens, la participation de Huawei au National Broadband Network, un gigantesque projet d'infrastructure public, à 40 milliards de dollars, visant à apporter le haut débit à 12 millions d'entreprises et de foyers australiens. Et pas plus tard qu'au printemps 2018, son gouvernement refusait qu'une filiale du groupe de Shenzhen relie par un câble sous-marin en fibre optique Sydney aux îles Salomon. Le gouvernement de ce petit État archipel du Pacifique planifiait pourtant l'établissement de ce lien depuis 2010, selon un communiqué publié par Huawei[4], pour enfin disposer d'une bande passante convenable qui ne repose pas sur des connexions satellitaires médiocres. Mais, à nouveau inquiet pour la sécurité d'une telle infrastructure, Canberra avait tué ce projet à plusieurs dizaines de millions de dollars, en interdisant l'atterrissement du câble sur ses côtes. Pour ne pas s'aliéner les îles Salomon, l'Australie avait même accepté de financer en grande partie le projet alternatif de Câble de la mer de Corail, reliant sur 4 700 km Sydney à la Papouasie-Nouvelle-Guinée, puis au petit archipel en mal de connectivité.

Sur tous ces dossiers, les recommandations des espions australiens étaient claires, mais jamais formulées publiquement. La 5G va les pousser à sortir de l'ombre. Le 29 octobre 2018, le compte Twitter officiel de l'Australian Signals Directorate (ASD), la branche Cyber des renseignements australiens, publie son tout premier message sur le réseau social : « Salut Internet, c'est l'ASD. Ça fait longtemps que j'écoute, c'est la première fois que j'appelle[5]. » Le

même jour, Mike Burgess – son patron et un des convives du dîner du 17 juillet – donne un discours à Canberra[6]. C'est une première en soixante et onze ans d'histoire pour l'ASD. Mike Burgess, un grand chauve aux oreilles décollées, connaît parfaitement le sujet 5G pour avoir longtemps été le directeur informatique de Telstra, le premier opérateur télécoms du pays. Devant les invités du « dîner sur la sécurité nationale » organisé par le think tank Australian Strategic Policy Institute (Aspi), il explique d'un ton rapide et tranchant : « La technologie 5G va sous-tendre les communications sur lesquelles vont reposer tous les Australiens, depuis nos systèmes de santé jusqu'aux applications émergentes de chirurgie à distance en passant par la fourniture d'eau et d'énergie. Les enjeux ne sauraient être plus élevés », avant de détailler pourquoi il a recommandé au gouvernement « d'exclure les fournisseurs à haut risque de la totalité des réseaux 5G ».

Les membres des Five Eyes ont-ils convenu de monter au créneau publiquement ? Une chose est sûre, leurs prises de parole vont se succéder après celle de Mike Burgess. Seuls les services secrets néo-zélandais ne feront pas d'apparition publique en cette fin d'année 2018, ce qui ne les empêchera pas, fin novembre, d'interdire officiellement à Spark, le premier opérateur du pays, de déployer des antennes 5G Huawei en raison des « risques de sécurité nationale[7] ».

Parmi les « Cinq Yeux », il ne reste alors que le Royaume-Uni et le Canada à ne pas s'être exprimés. Leurs maîtres espions vont sortir de l'ombre début décembre, à vingt-quatre heures d'intervalle. Le premier sera le patron du MI6, Alex Younger. Celui que l'on désigne, comme tous ses prédécesseurs à cette fonction, de la simple lettre C fait alors sa deuxième apparition publique depuis son entrée en fonction quatre ans plus tôt. Il a réservé cet honneur aux étudiants de son ex-université, la prestigieuse St Andrews – troisième plus

ancienne université anglophone, après Oxford et Cambridge. Les vieilles pierres écossaises se prêtent aux confidences et le patron du MI6 raconte de bonne grâce ses débuts d'agent infiltré pendant les guerres de Yougoslavie des années 1990 et les « nombreuses nuits à boire d'obscurs alcools faits maison[8] ». Interrogé sur la 5G, Alex Younger apparaît plus mesuré que ses homologues avec qui il dégustait des homards six mois plus tôt. « Nous devons décider dans quelle mesure nous serons à l'aise avec le fait que les Chinois soient propriétaires de ces technologies et de ces plateformes dans un environnement où certains de nos alliés ont pris une position plutôt ferme, explique le Britannique. Il faut que nous ayons un débat. Ce n'est pas si simple. » Outre que trois des quatre opérateurs du pays ont déjà des antennes Huawei dans 40 à 60 % de leurs réseaux, le Royaume-Uni surveille depuis huit ans le fonctionnement de Huawei grâce aux employés de The Cell – le bâtiment de la banlieue d'Oxford où sont disséqués tous ses produits[*2]. Et si ceux-ci déplorent rapport après rapport des vulnérabilités importantes et des méthodes de développement insuffisamment rigoureuses, ils n'ont jamais mis en évidence des pratiques d'espionnage ou de risque majeur pour la sécurité globale des réseaux. Ren Zhengfei estimera lui-même que « s'ils détectent des problèmes, c'est tout à fait normal. Je ne dis pas qu'il n'y a aucun problème avec nos équipements, je dis simplement qu'il n'y a rien de malveillant dans ces équipements[9] ».

Moins d'une semaine après le speech de C toutefois, BT fait une annonce importante. L'opérateur historique britannique – soutien de longue date de Huawei, qu'il a propulsé dans la cour des grands – va retirer les équipements du constructeur chinois de ses cœurs de réseau 3G et 4G – la partie amont du réseau mobile, où sont gérées les informations sensibles sur l'identité et l'activité des clients. Et BT conservera cette distinction pour ses appels d'offres 5G : Huawei ne

pourra pas fournir les cœurs de réseau et sera cantonné au réseau d'accès radio, c'est-à-dire aux antennes, jugées moins sensibles. Cette distinction entre le « cœur » et la « périphérie » du réseau est une élégante façon de couper la poire en deux. Mais elle ne convainc pas tout le monde. En Australie, le patron de l'ASD Mike Burgess a publiquement expliqué, quelques mois plus tôt, que cette frontière n'était absolument pas pertinente avec la 5G. À un responsable des affaires publiques de Huawei Australie qui lui assurait le contraire, le patron des cyber-espions australiens s'est même permis une réponse lourde de sous-entendus sur Twitter : « Dans mon activité, je n'ai jamais rien vu de "complètement isolé"[10]… »

Un an plus tard, c'est pourtant l'approche qui sera retenue par le Premier ministre britannique Boris Johnson : autoriser Huawei pour la 5G, dans la limite de 35 % du marché et à l'exclusion des cœurs de réseau. Le groupe de Shenzhen s'en félicitera chaudement. Comparée aux affronts des autres Five Eyes, cette moitié de feu vert est déjà une grande victoire.

Étonnamment, le seul membre de l'alliance à ne pas avoir pris position sur Huawei est le Canada, c'est-à-dire le pays qui accueillait la réunion des espions à l'été 2018. Le 4 décembre, un jour après Alex Younger, son homologue des services secrets canadiens David Vigneault a lui aussi pris la parole publiquement pour la première fois[11]. Le patron du Canadian Security Intelligence Service a mis en garde contre l'espionnage de certains États dans des domaines essentiels, et notamment la 5G[12]. Mais il n'a donné ni de nom de pays, ni de nom d'entreprise. Ce n'est sans doute pas une coïncidence si, trois jours plus tôt, Meng Wanzhou a été arrêtée à Vancouver. Le grand public n'est pas encore au courant, mais l'affaire embarrasse déjà au plus haut point les autorités d'Ottawa.

Le pari de Rakuten

Il n'y a pas qu'au sein du petit cercle des Five Eyes que le débat sur la 5G monte en puissance. Pressé par son allié américain, le Japon est le premier pays en dehors du monde anglo-saxon à fermer la porte aux équipementiers chinois fin 2018. Légalement, le gouvernement se contente de demander aux opérateurs de l'archipel de prendre en compte les questions de cybersécurité dans les processus d'approvisionnement. Mais le résultat est le même. Les trois groupes qui se partagent le marché nippon ont compris le message subliminal et font tous l'impasse sur les fournisseurs chinois. Même Softbank tourne le dos à Huawei, son partenaire de longue date. Le numéro 3 japonais est la propriété du milliardaire Masayoshi Son – sorte de prophète de la tech mondiale depuis qu'en 2016 il a constitué un fonds de 100 milliards de dollars pour investir dans les paris les plus futuristes. « Masa » a-t-il vu dans sa boule de cristal ce que l'avenir réservait à son fournisseur de Shenzhen ? Pour la deuxième fois, il lui fait en tout cas un coup de Jarnac. En 2013, le petit homme au flair légendaire – il a notamment investi avant tout le monde dans deux entreprises encore minuscules à l'époque, Yahoo ! et Alibaba – s'était lancé dans l'ambitieux rachat du troisième opérateur mobile américain, Sprint. Et pour s'attirer les bonnes grâces des régulateurs, il n'avait pas hésité alors à promettre que le réseau de Clearwire – un petit opérateur sur lequel Sprint était au même moment en train de mettre la main – serait bientôt débarrassé des équipements Huawei. L'affaire sera conclue, prouvant que l'entrepreneur avait raison de brosser les politiques dans le sens du poil. Cinq ans après ses intrigues pour racheter Sprint, Masayoshi Son a compris qu'il lui faut maintenant couper les ponts avec le champion chinois même au Japon.

Malgré ces revers, Huawei avait un dernier joker sur le marché japonais. Un quatrième groupe, le spécialiste du commerce en ligne Rakuten, avait en effet décidé de profiter de la 5G pour se lancer dans les télécoms. Le pari était osé. Il fallait bâtir un réseau mobile national en partant de zéro, avec le seul avantage d'être libre de toutes les contraintes habituellement liées à une architecture historique. Pour ce faire, quel meilleur partenaire que le numéro 1 mondial des télécoms – notoirement en avance sur la technologie 5G ? Au printemps 2018, Huawei est sur le point de remporter ce contrat pas comme les autres. Mais dans la dernière ligne droite, le deal capote[13]. Rakuten décide finalement de faire un pari encore plus fou. Le nouvel entrant va tester une autre architecture de réseau, baptisée Open-RAN (pour « réseau d'accès radio ouvert »). Cette alternative aux solutions des grands fournisseurs tels que Huawei, Ericsson ou Nokia consiste à remplacer leurs équipements par de simples serveurs tels qu'on en trouve dans n'importe quelle salle informatique de la planète, et de les munir de logiciels remplissant toutes les fonctions d'un équipement télécoms traditionnel. La perspective est très séduisante pour les opérateurs : elle est synonyme de matériel moins cher, car générique, mais aussi d'une plus grande concurrence et d'une meilleure interopérabilité entre fournisseurs des différents logiciels de gestion des réseaux et des antennes. « C'est le Graal, mais cela reste à tester sur le terrain[14] », explique dans *Les Échos* à propos d'Open-RAN Tariq Ashraf, consultant chez Bearing Point et excellent connaisseur du secteur. Le défi technique est gigantesque et, si tous les grands opérateurs – comme Vodafone ou Orange – mènent des tests, nul industriel n'est encore prêt à se lancer dans une expérience grandeur nature. Le risque est trop grand que la qualité ne soit pas au rendez-vous et chacun préfère attendre que la technologie Open-RAN se rode encore quelques années avant de se

jeter à l'eau. La décision audacieuse de Rakuten de tout miser sur Open-RAN dès 2018 provoque quelques haussements de sourcils dans les états-majors des grands opérateurs de la planète. Mais tous enverront des équipes au Japon dans les mois suivants pour étudier cette grande première. Au printemps 2020, quand Rakuten allume son réseau, la circonspection reste de mise. L'opérateur a beau vanter des coûts fixes réduits de moitié par rapport à un réseau traditionnel, chacun attend encore de voir si ce gigantesque projet à plus de 5 milliards de dollars tient la charge dans la durée. Pour Huawei en tout cas, la punition est double. Non seulement l'intégralité du marché japonais lui a échappé, mais en plus cette éviction a sans doute précipité l'avènement d'Open-RAN, une technologie qui ambitionne de ringardiser les équipementiers traditionnels. Ce n'est sans doute pas une surprise d'ailleurs si les États-Unis soutiennent à toute force Open-RAN. Alors que ses anciennes gloires des télécoms – Nortel, Motorola, Lucent… – ont vécu, c'est une occasion en or pour l'Amérique de revenir dans le jeu par une porte dérobée. De nombreuses petites entreprises américaines sont sur les rangs : Mavenir, Altiostar, Parallel Wireless… C'est également le cas de plusieurs fleurons déchus des télécoms japonais, comme NEC et Fujitsu, qui misent ouvertement sur Open-RAN et ne peuvent que se féliciter d'être remis en selle par les tensions sino-américaines.

L'Europe entre deux chaises

Fin 2018, en dépit des portes qui se sont fermées en Australie, en Nouvelle-Zélande et au Japon, Huawei peut relativiser. Ces revers très médiatisés ont une portée symbolique plus qu'un véritable impact économique sur les résultats du groupe. Le champion chinois de la 5G

sait que c'est l'Europe qui constitue la pièce maîtresse de sa grande partie d'échecs avec Washington. Le Vieux Continent est son deuxième marché après la Chine. En dehors de l'Afrique – où ses équipements sont omniprésents –, c'est aussi sa meilleure implantation à l'international. Une étude du cabinet danois Strand[15] détaille la présence des équipements chinois dans les réseaux 4G des opérateurs de 31 pays européens (les membres de l'Union européenne, la Norvège, la Suisse et les îles Féroé). Le résultat est impressionnant. 44 % des consommateurs européens reçoivent leur signal 4G d'une antenne Huawei – largement plus que n'importe quel autre fournisseur. En ajoutant ZTE, on arrive à une part de marché de 48 %. Dans trois pays européens, l'intégralité des réseaux 4G est constituée d'antennes chinoises. Il est intéressant de noter que c'est notamment le cas de la Belgique, siège des institutions de l'Union européenne, où les trois opérateurs sont soit 100 % équipés par Huawei (Orange Belgique et Proximus), soit 100 % par ZTE (Telenet). Ce succès phénoménal avec les réseaux 4G peut-il être renouvelé avec l'arrivée de la 5G ? Les Chinois comptent sur leur emprise historique, en plus de leur savoir-faire technologique, pour s'imposer.

Huawei peut aussi se prévaloir de son poids économique dans la région. Il emploie quelque 11 000 salariés en Europe, dont près de 2 000 sur des activités très prisées de R&D. Le départ d'un tel acteur ne serait pas sans conséquences. En Australie, d'où Huawei a été écarté dès 2018, l'entreprise a dû se résoudre à se séparer de plus de 80 % de ses 1 200 salariés. Elle a mis fin à ses divers contrats de partenariat de recherche – représentant 100 millions de dollars australiens (environ 60 millions d'euros) –, a dissous son conseil d'administration local et retiré son soutien financier au club de rugby de Canberra – qui se traduisait par un grand logo rouge sur la

poitrine des joueurs au maillot vert et, selon la presse locale, plus d'un million de dollars australiens (environ 600 000 euros) par an pour le club[16]. Les pays européens connaissent ces enjeux. Mais cela ne va pas suffire à contenir l'incendie allumé par Washington.

Contre toute attente, le premier départ de feu sera signalé en République tchèque. Prague est plutôt réputé proche de Pékin, et la quasi-totalité des réseaux mobiles du pays est équipée par Huawei. Mais le 17 décembre 2018, cela n'empêche pas le patron du Nukib – les services de cybersécurité tchèques – de jeter un pavé dans la mare, en lançant un « avertissement[17] » officiel contre l'utilisation des matériels et logiciels de Huawei et de ZTE. Le premier des cyber-espions tchèques, Dušan Navrátil – à qui un visage rond, des petites lunettes et une moustache en brosse fournie donnent plutôt l'allure d'un grand-père débonnaire –, affirme n'avoir pas eu d'autre choix après avoir réuni des éléments en interne et auprès de ses alliés, mais également analysé l'environnement juridique et politique de la République populaire de Chine[18]. Techniquement, l'avertissement des services tchèques ne fait que contraindre les opérateurs télécoms et autres gestionnaires d'infrastructures critiques à réaliser une analyse des risques, rien de plus. Mais politiquement, c'est une bombe pour les autorités tchèques, et notamment pour le président Miloš Zeman. À la tête de l'État depuis 2013, ce vieux briscard de la politique a orchestré un grand rapprochement avec Pékin pour attirer les investissements chinois dans son pays. Pas franchement enchanté par la sortie de Dušan Navrátil, le président tchèque ne tarde pas à désavouer le rapport de ses services secrets. Il va même jusqu'à rassurer Ren Zhengfei en personne, en Chine, au printemps suivant. Le site de Huawei se fait l'écho de cette rencontre au sommet, avec un court article, illustré par une photo de la poignée de main entre les deux hommes. Miloš Zeman y assure que les accusations contre

Huawei sont « sans fondement » et espère voir « la poursuite du développement de Huawei en République tchèque[19] ». Neuf mois plus tard, Dušan Navrátil est brutalement démis de ses fonctions[20]. Mais le départ du directeur du Nukib n'éteint pas complètement les braises de son « avertissement ». En réalité, au milieu d'un invraisemblable imbroglio politico-économique, où se mêlent la rivalité entre le président et son Premier ministre Andrej Babiš et une série de déceptions liées à de gros investisseurs chinois peu fiables, personne n'est au clair sur les intentions de Prague concernant Huawei. Et personne ne le sera ni en 2019, ni en 2020.

Ce tiraillement entre les enjeux économiques, politiques et sécuritaires caractérise la position de l'Europe en général. Pris dans des injonctions contradictoires, les pays de l'Union sont désemparés. En tant que première puissance économique du bloc, l'Allemagne n'est pas la moins pétrifiée. La chancelière Angela Merkel ne cache pas sa réticence à céder aux pressions américaines et à exclure les fournisseurs chinois de ses marchés 5G. Les opérateurs allemands sont tous de grands clients de Huawei et n'hésitent pas à faire valoir qu'un changement de fournisseur serait coûteux – en investissement et en temps. L'argument est relayé par la puissante industrie allemande, notamment le secteur automobile, qui attend énormément des promesses d'automatisation de la 5G – beaucoup plus que la majorité des entreprises européennes. Au même moment en France, Sébastien Soriano, le patron de l'Arcep, le régulateur des télécoms, désespère par exemple de ne voir aucun grand industriel tricolore répondre à son appel pour équiper en 5G un port, une usine ou un hôpital. Alors quand son homologue allemand lui fait part de ses « difficultés », le Français met un long moment à comprendre que de l'autre côté du Rhin, c'est tout le contraire : les grands groupes font le siège de la Bundesnetzagentur pour accélérer au maximum le

processus d'attribution des fréquences, dont ils ont même négocié de réserver une partie aux seuls industriels. Angela Merkel sait que pour garder la place de choix de l'Allemagne dans la compétition mondiale, elle ne peut pas faire prendre du retard au pays dans l'adoption de la 5G. Elle sait aussi que la Chine est un de ses premiers marchés à l'export, dont elle ne peut se permettre de s'aliéner les autorités. Enfin, elle fait une analyse des risques sensiblement différente de celle des États-Unis. Elle dévoilera en partie sa pensée, début 2020, au forum de Davos. Sans jamais nommer Huawei ou la Chine, « Mutti » explique alors que la meilleure des sécurités en matière de 5G réside dans la diversification et la redondance. « Je ne pense pas me rendre particulièrement sûre si j'élimine des fournisseurs dans leur totalité et ne sais pas ensuite comment ils se développent », explique la dirigeante allemande.

Mais sa ligne est loin de faire l'unanimité dans son pays. Ce n'est même pas un problème politique. Des élus des deux bords font pression pour se passer de fournisseurs « sujets à l'influence d'une puissance étrangère ». Au sein de la CDU, le propre parti d'Angela Merkel, la fronde est très vive. Et Washington ne se prive pas d'alimenter la zizanie dès que l'occasion se présente. Début mars 2019, une lettre de Richard Grenell, l'ambassadeur américain en Allemagne connu pour ses diatribes peu diplomatiques, fuite dans le *Wall Street Journal*[21]. Elle est adressée au gouvernement allemand et, pour la première fois, fait ouvertement planer la menace d'un ralentissement des échanges de renseignements entre Berlin et Washington, si d'aventure Huawei était autorisé à participer à la 5G allemande. En pleine psychose terroriste en Europe – et alors que les combats pour faire tomber l'État islamique font encore rage en Syrie –, la lettre est interprétée par beaucoup comme un grossier chantage. Elle agace en tout cas Berlin. « Nous définissons nos

propres standards » pour la sécurité des réseaux 5G, martèle quelques jours plus tard Angela Merkel devant la presse. Ce qui n'empêchera pas Washington de poursuivre ouvertement son travail de sape. En mai, c'est carrément Mike Pompeo – le secrétaire d'État américain et prédécesseur de la redoutable Gina Haspel à la tête de la CIA – qui s'y colle. En déplacement officiel à Berlin, cet ex-officier qui « patrouillait le rideau de fer avant la chute du mur de Berlin[22] » renouvelle la menace : pas de Huawei, ou c'en est fini des bons tuyaux de l'Oncle Sam.

Un amendement anti-Huawei

L'ultimatum ne vise pas que l'Allemagne. Assis dans la bibliothèque de l'ambassade américaine à Paris le 22 janvier 2020, Robert Strayer tient le même langage que son patron, enrobé de quelques circonvolutions : « Nous avons des échanges d'informations très solides avec la France […]. S'il y a des réseaux non sécurisés de fournisseurs non fiables qui pourraient compromettre les données que nous échangeons, cela pourrait aisément compromettre le tempo opérationnel de nos opérations communes, notre capacité à partager des informations dans des délais appropriés. » Les États-Unis maintiennent la pression sur la France, car Huawei n'a pas été formellement exclu de la 5G tricolore. Mais en réalité, Washington n'est pas mécontent de la tournure qu'ont prise les choses dans l'Hexagone. Paris a géré le dossier de façon à bannir Huawei sans le dire – une leçon d'esquive diplomatique. L'affaire n'avait rien d'évident pour les autorités. Huawei emploie plus de 1 000 personnes en France. C'est un gros client de certains groupes français, comme STMicro. Huawei a acheté pour plus de 700 millions de produits

tricolores en 2018. Ses antennes équipent par ailleurs la moitié des réseaux de Bouygues Telecom et de SFR. Patrick Drahi, le milliardaire propriétaire de SFR, est même tellement content du rapport qualité-prix des équipements chinois, qu'en 2018, il est sur le point d'abandonner Nokia pour confier tout son réseau à Huawei[23]. Selon des sources gouvernementales, c'est d'ailleurs cette ambition de Patrick Drahi qui va précipiter les choses.

Depuis des années, un accord tacite a été conclu entre l'État et les opérateurs français. Ils peuvent utiliser le matériel chinois, mais pas dans les cœurs de réseau, pas en région parisienne, et pas sur plus de 50 % de leur infrastructure. La volonté de SFR de passer en force en s'asseyant sur ce *gentlemen's agreement* va forcer Paris à clarifier les règles. Selon plusieurs sources concordantes, Emmanuel Macron est lui-même un partisan d'une ligne dure face à la Chine, et face à Huawei en particulier. Du temps où il était ministre de l'Économie, il n'a pas manqué de le faire savoir à Martin Bouygues et à Patrick Drahi. Maintenant qu'il est installé à l'Élysée et que l'arrivée prochaine de la 5G augmente les enjeux, il compte bien fermer la porte aux équipements chinois. Mais pas question de le clamer haut et fort. Le président français n'est pas crâne au point de risquer un conflit frontal avec Pékin, qui coûterait cher aux exportateurs français de produits agricoles, de luxe, d'aéronautique ou de nucléaire. L'idée qui a émergé à l'Élysée, et qui sera présentée aux opérateurs lors d'une réunion à Bercy le 16 janvier 2019, est d'étendre les pouvoirs de l'Anssi qui dépend, *in fine*, de Matignon – pour exiger son feu vert avant toute installation de matériel dans l'Hexagone. Bouygues et SFR sont furieux. Ils ont vite compris l'entourloupe. Officiellement, l'État va pouvoir continuer à assurer que tous les équipementiers sont les bienvenus en France. Mais l'Anssi fera en sorte de bloquer les dossiers d'autorisation de Huawei et, à force de tracasseries

administratives, les opérateurs finiront d'eux-mêmes par abandonner leur fournisseur chinois. L'ambassade de Chine en France n'est pas dupe non plus, et prévient dans un communiqué qu'« une différence de traitement des entreprises selon leur pays d'origine constituera une discrimination patente et un protectionnisme déguisé », avant de menacer de rétorsions, en termes à peine voilés, Nokia et Ericsson en Chine, mais aussi le nucléaire, l'aéronautique et l'aérospatial français[24].

Le gouvernement n'en a cure. Facialement, il est parfaitement neutre. Pour verrouiller le dispositif, les cabinets ministériels bricolent en urgence un amendement – rapidement baptisé « anti-Huawei » par tous les observateurs même si le texte fait bien attention à ne jamais pointer du doigt une entreprise en particulier. Après un léger bras de fer avec le Sénat, mécontent d'être ainsi mis au pied du mur, le texte revient sous la forme d'une proposition de loi sur la « sécurité des réseaux mobiles », votée sans difficultés à l'été 2019. Selon les nouvelles règles du jeu, les opérateurs notifieront désormais l'Anssi de tout projet d'installation, qui doit donner son accord. Pendant près d'un an, les opérateurs continueront à pester de ne pas savoir ce qui sera autorisé. Le patron de l'Anssi, Guillaume Poupard, douchera leurs derniers espoirs de continuer à utiliser Huawei dans une interview aux *Échos* début juillet 2020. À la question de savoir si ses services ont refusé des antennes Nokia ou Ericsson, le fonctionnaire répond simplement « Non ». Et concernant leur concurrent chinois, il précise : « Les opérateurs qui n'utilisent pas Huawei, nous les incitons à ne pas y aller car c'est un peu le sens naturel des choses. Ceux qui l'utilisent déjà, nous délivrons des autorisations dont la durée varie entre trois et huit ans. » On peut difficilement être plus cash à ce niveau de responsabilités. Dans les grandes villes, Huawei est banni *de facto* pour divers motifs de sécurité – la protection des usines

Airbus à Toulouse, celle des bases de sous-marins à Brest… L'équipementier chinois n'est autorisé que dans les zones périphériques – ce qui est difficilement gérable par les opérateurs qui fonctionnent d'ordinaire avec un seul fournisseur sur toute une zone géographique. Pire, ses équipements ne sont autorisés que pour une durée limitée, et les autorités laissent entendre que ces autorisations ne seront pas renouvelées. La messe est dite. Sans jamais l'écrire, Paris a fermé la porte à Huawei.

À Bruxelles, la Commission européenne observe ces mouvements avec beaucoup d'embarras. Elle aimerait que l'Union européenne adopte une position commune, mais la sécurité nationale est du ressort des États membres – et leurs décisions partent dans tous les sens. Certains, comme le Portugal, l'Espagne ou la Roumanie ouvrent largement leurs portes à Huawei. L'Angleterre transige, la France finasse, l'Allemagne hésite. Mi-2019, pour tenter de regrouper ce troupeau égaré, l'exécutif européen fait comme à son habitude… et commande un rapport. Présentée le 9 octobre à la presse, cette « évaluation des risques de cybersécurité liés à la 5G » ne suscite qu'une question lancinante dans la salle : « Pourquoi ne citez-vous pas Huawei ? » Car après avoir détaillé l'ampleur des risques nouveaux qui vont apparaître avec la 5G, le texte appelle les États membres à la vigilance face à des fournisseurs avec des liens forts avec le gouvernement d'un pays tiers, une structure actionnariale particulière ou opérant dans un pays sans contre-pouvoirs démocratiques. La description est générique, mais qui peut faire semblant de ne pas voir le groupe de Shenzhen dans le portrait en creux fait par Bruxelles ? Quelques mois plus tard, la Commission européenne dévoilera une « boîte à outils » sur la 5G à l'intention des États membres. Tout aussi neutre que le rapport initial dans sa présentation, elle a surtout le mérite d'obliger les pays du bloc à

ouvrir un débat sur leurs fournisseurs 5G et à en rendre compte à Bruxelles. Mais, diplomatiquement et politiquement, l'exécutif européen ne peut pas aller beaucoup plus loin.

Les leviers chinois

Pendant que les États-Unis mettent dans la balance les précieux renseignements de leurs services secrets, la Chine multiplie les menaces commerciales pour défendre son champion de la 5G. Et c'est bien malgré lui que Helgi Abrahamsen, le ministre du Commerce des îles Féroé, va le révéler au monde. Le 15 novembre 2019, il est dans les locaux de la chaîne de télévision locale, Kringvarp Føroya, pour une interview sur Huawei, précisément, qui équipe en totalité les réseaux 4G de l'archipel. Comme partout en Europe, la question de sa participation à la 5G est dans toutes les têtes. Le ministre va habilement éviter de répondre aux questions qui fâchent, en bon politique rodé aux médias. Seulement, un peu avant de passer à l'antenne, il s'entretient brièvement, dans une salle à part, avec son directeur de cabinet. Le ministre est déjà équipé de son micro-cravate, mais il ne s'est pas rendu compte que celui-ci est ouvert et que sa conversation est enregistrée. Le journal danois *Berlingske* en révélera le contenu le 11 décembre, après que le gouvernement féringien a tenté d'empêcher juridiquement la diffusion du clip audio[25]. Le ministre y discute des menaces ouvertement proférées auprès de plusieurs membres du gouvernement par l'ambassadeur de Chine au Danemark d'abandonner un projet de libre-échange, critique pour l'industrie locale de la pêche au saumon, si Huawei n'obtenait pas l'autorisation de construire les réseaux 5G.

Le gouvernement des îles Féroé et le ministère chinois des Affaires étrangères démentiront toute forme de pression. Mais trois jours plus tard, c'est au tour de l'ambassadeur de Chine à Berlin de faire des remarques plus qu'ambiguës. « Si l'Allemagne devait prendre une décision qui conduise à l'exclusion de Huawei du marché allemand, il y aura des conséquences. Le gouvernement chinois ne restera pas les bras croisés[26] », lance Ken Wu. En rappelant à son auditoire qu'un quart des 28 millions de voitures vendues en Chine l'année précédente étaient allemandes, le diplomate fait semblant de s'interroger : « Pouvons-nous dire que les voitures allemandes ne sont pas sûres parce que nous sommes en mesure de produire nos propres voitures ? Non, ce serait du pur protectionnisme. »

Bien que Huawei ne soit pas une entreprise publique, Pékin ne ménage pas sa peine pour défendre le groupe. Ce qu'Eric Xu, un des vice-présidents tournants du groupe, justifiera dix-huit mois plus tard lors de la présentation des résultats annuels, par une formule choc : « Le gouvernement chinois ne va pas rester à ne rien faire pendant que Huawei se fait massacrer sur une planche à découper. » D'ailleurs, quel gouvernement ne défend pas les intérêts de ses fleurons technologiques à l'étranger ? Le problème – et les autorités canadiennes en sont douloureusement convaincues depuis déjà un an –, c'est que la Chine est prête à aller très loin dans la défense de ces intérêts.

Le 10 décembre 2018, une semaine après l'arrestation de Meng Wanzhou à Vancouver, deux Canadiens se sont en effet retrouvés, bien malgré eux, embarqués dans le grand thriller de la 5G. Le premier est un ancien diplomate de quarante-six ans qui travaille en Chine comme analyste pour l'International Crisis Group, une ONG de prévention des conflits active sur tous les points chauds du globe – parfois au péril de leur vie. Parlant parfaitement mandarin, Michael

Kovrig intervient régulièrement dans les médias chinois et anglo-saxons. Le second a un profil plus baroque. Depuis vingt ans, Michael Spavor organise des échanges et des voyages à destination de la Corée du Nord, dont il connaît intimement l'étrange dictateur Kim Jong-un. Une photo, publiée en 2013 par le compte Instagram de son organisation, Paektu Exchanges, montre les deux hommes sirotant un cocktail en tête à tête, sur le yacht du dirigeant nord-coréen. La même année, Michael Spavor a organisé le voyage à Pyongyang de Dennis Rodman, la star de la National Basketball Association (NBA) américaine. Résidant à l'année de l'autre côté de la frontière marquée par le fleuve Yalou, dans la ville chinoise de Dandong, Michael Spavor a prévu, en cette deuxième semaine de décembre 2018, de se rendre à Séoul pour le travail. Il n'y arrivera jamais. À quelques heures d'intervalle, la police chinoise appréhende les deux Michael, l'un à Dandong, l'autre à Pékin. Emprisonnés en un lieu indéterminé, sur de vagues accusations d'atteinte à la sécurité de l'État, les deux hommes sont interrogés matin, midi et soir, selon des diplomates canadiens, maintenus à l'isolement dans deux cellules où la lumière n'est pas éteinte la nuit, sans accès à un avocat. Ce n'est que six mois plus tard que les charges d'espionnage seront officiellement annoncées, provoquant la consternation à Ottawa, où Justin Trudeau dénonce une « arrestation arbitraire ». Le gouvernement canadien est convaincu que la Chine a pris les deux hommes en otage pour faire pression dans le dossier de Meng Wanzhou et de Huawei. Malgré les dénégations de Pékin, qui jure qu'il n'y a aucun rapport, le Canada sera encore plus convaincu lorsque, quelques semaines plus tard, un Canadien, jugé en appel par la justice chinoise pour trafic de drogue, après avoir été condamné à quinze ans de prison en première instance, est condamné à mort, à la stupeur générale. L'affaire sera très médiatisée en Chine, et la photo du malheureux Robert

Schellenberg – un frêle trentenaire au teint blanc et au crâne dégarni –, assis dans son box entre deux officiers de police chinois, fera le tour du monde.

En plus de ces drames isolés, le Canada doit aussi encaisser des attaques commerciales de la Chine. Au printemps 2019, c'est d'abord un quasi-embargo chinois qui est annoncé sur son colza – une plante utilisée dans la fabrication d'huile et de biocarburant, dont il est le premier producteur mondial. La Chine engloutit d'ordinaire la moitié de la production canadienne et les agriculteurs des grandes plaines jaunes de l'Alberta ou du Saskatchewan se retrouvent pris à la gorge. Peu de temps après, c'est au tour du porc canadien, puis de tous ses produits carnés de se voir interdire de passer les frontières chinoises. Pour justifier cet embargo, Pékin invoque la découverte de 190 faux certificats d'exportation accompagnant une cargaison de viande canadienne. À Ottawa, si l'on ne nie pas ce problème sanitaire, la réaction est jugée disproportionnée et les Canadiens, en dépit des dénégations chinoises, ne peuvent s'empêcher d'y voir des mesures de rétorsion à l'arrestation de Meng Wanzhou.

Pris à partie par sa population face à cette avalanche de mauvaises nouvelles, Justin Trudeau refuse pourtant d'intervenir dans le processus d'extradition. Le Premier ministre juge contreproductif et même dangereux pour les millions de Canadiens qui vivent ou voyagent à l'étranger de céder au chantage. Un an après l'arrestation de Meng Wanzhou, il reconnaîtra dans l'émission télévisée *Salut bonjour*[27] que « c'est très long pour les Canadiens qui sont détenus » et qu'il essaie de faire comprendre aux Chinois, qui ont « un système très différent », que ce n'est pas « une façon d'aider leur cause ». Mais fin 2020, force est de constater qu'il n'y est pas parvenu. Les deux Michael entament leur troisième année au fond des geôles chinoises ; Meng Wanzhou, sa troisième année dans sa

ravissante demeure de Vancouver où la justice l'a contrainte à résider, une balise GPS à la cheville.

La facture

Les opérateurs télécoms ont tendance à regarder la question de leurs équipements – et c'est bien naturel – sous un prisme technique et économique. Les histoires de politique commerciale internationale, de possibles prises d'otages ou de pirates sponsorisés par des États ne sont pas des éléments à faire valoir devant un conseil d'administration. De leur point de vue, Huawei est un excellent fournisseur, à la fois par la qualité de ses produits et de ses services, qui n'a jamais été pris en défaut sur des questions de sécurité. Les États-Unis peuvent bien accuser Huawei de tous les crimes du monde, ils n'ont pas apporté le début d'une preuve que Pékin se servait de son champion national des télécoms pour espionner ou saboter les infrastructures de pays tiers. Dès lors, pourquoi s'en passer ? D'autant que les consignes des autorités sont loin d'être claires. « On dit des choses publiquement, on ne dit jamais de nom et dès qu'on a le dos tourné, on nous passe des messages, donc cette espèce de duplicité, c'est pénible[28] », s'emporte Stéphane Richard, le patron d'Orange, début 2020.

Ce que les opérateurs redoutent, en particulier en Europe, c'est le coût d'une exclusion de Huawei des marchés 5G. Ils savent qu'il est très compliqué de faire fonctionner les équipements de deux fournisseurs différents sur un même site – par exemple une antenne 5G d'Ericsson sur un pylône qui accueille déjà des antennes 3G et 4G de Huawei. Faire une croix sur la 5G de Huawei, pour les opérateurs qui font appel à lui pour les générations de réseaux précédentes, cela

revient à tout mettre à la poubelle. En France par exemple, Bouygues Telecom et SFR – dont la moitié du réseau mobile est constitué d'antennes chinoises – expliquent à qui veut l'entendre que ce serait un gouffre financier, sans aller jusqu'à avancer un chiffre. Tout juste pointent-ils que les États-Unis ont prévu de débourser 2 milliards de dollars rien que pour dédommager leurs petits opérateurs ruraux qui, contrairement aux quatre grands, AT&T, Verizon, Sprint et T-Mobile, étaient souvent équipés de matériel chinois. En Europe, les estimations de la facture d'une exclusion de Huawei varient de 3 milliards d'euros à plus de 55 milliards selon les études… Dans *Les Échos*, un expert du secteur fait le calcul suivant : en comptant 100 000 euros pour un pack d'antennes – et en prenant en compte que leurs parcs d'environ 20 000 pylônes sont largement mutualisés –, Bouygues et SFR devraient signer un chèque de 500 à 700 millions d'euros chacun afin d'expurger leurs réseaux de tout matériel chinois[29]. Et encore, cela n'intègre pas les coûts indirects liés aux inévitables départs de clients à cause des perturbations sur le réseau…

L'équation, déjà complexe, est encore bousculée quand les États-Unis décident, à l'été 2020, de fermer le robinet mondial des puces électroniques à Huawei. Le fait que Washington déclenche cette « option nucléaire[*3] » fait, pour la première fois, peser un risque existentiel sur le groupe de Shenzhen. Huawei fera tout pour rassurer ses clients, allant, selon des sources de l'industrie, jusqu'à financer et stocker des mois d'équipements d'avance. Mais ce qui n'était qu'un risque politique – celui d'être exposé à une interdiction administrative – est devenu un risque industriel – celui de voir son fournisseur mettre la clé sous la porte. Pire, pour les experts britanniques de The Cell, c'est aussi un risque de sécurité.

Revirement britannique

À l'été 2020, alors que les États-Unis ont privé *de facto* Huawei de tout approvisionnement en puces, le NCSC revoit en urgence sa copie. Contrairement à ce qu'il écrivait six mois plus tôt, il ne s'estime plus en mesure d'assurer la sécurité des réseaux 5G qui incluraient des produits Huawei. Son analyse est qu'en étant privé de puces américaines, le groupe de Shenzhen sera contraint de se rabattre sur des technologies moins connues, moins sûres et moins facilement contrôlables par les services de Sa Majesté. Ce raisonnement débouche sur une décision radicale. Boris Johnson renonce à ménager la chèvre et le chou, comme il l'escomptait encore en janvier. Plus question de limiter Huawei à la périphérie du réseau ou à 35 % du marché. En plein cœur de l'été 2020, le Premier ministre britannique franchit le Rubicon et annonce l'exclusion de Huawei de son marché. Tous les opérateurs du royaume devront cesser d'acheter le moindre matériel au groupe chinois dès la fin de l'année et devront démonter les infrastructures existantes d'ici 2027. La volte-face de Boris Johnson est un coup de tonnerre. Huawei pouvait jusqu'alors se vanter d'avoir la confiance du Royaume-Uni, le pays qui connaissait vraisemblablement le mieux ses produits grâce aux experts de The Cell. En 2005, la loyauté de BT lui avait ouvert les portes de l'Europe. En 2020, celle de Londres lui laissait ouverte l'entrée de nombreux pays. Bien des capitales pouvaient tenir le raisonnement suivant : si le premier allié de Washington continue d'utiliser Huawei, pourquoi pas moi ? L'argument vient de se retourner brutalement.

L'automne 2020 est une hécatombe pour Huawei. La Belgique lui tourne le dos, l'Allemagne prépare un durcissement des autorisations « à la française », la Suède l'abandonne… Au Département d'État américain, on se frotte les mains. « En février dernier, Huawei

annonçait qu'ils avaient 90 contrats 5G. Et ce que nous avons vu, c'est que ces contrats se sont évaporés. Au maximum, nous en comptons six en dehors de Chine[30] », assure Keith Krach le 30 septembre. Cet ancien patron d'une entreprise de logiciels a repris la mission de Robert Strayer, parti dans le privé après deux années à sillonner le globe pour faire dérailler Huawei. Et il a la partie plus facile que son prédécesseur, puisqu'il n'a plus qu'à constater que « le vent a complètement tourné ». Huawei, de son côté, ne donne pas de nouveaux chiffres.

En plus de se faire souffler l'Europe, le groupe commence à être en difficulté dans certains pays émergents. Si l'Afrique reste fidèle, l'Inde lui a discrètement claqué la porte au nez fin août, selon le *Financial Times*[31], priant ses opérateurs de ne plus utiliser d'équipements chinois. Le coup est rude. Avec 850 millions de clients, l'Inde est le deuxième marché mobile du monde après la Chine. Huawei y était solidement installé, non seulement avec ses activités de recherche à Bangalore, mais aussi avec de très gros contrats signés par deux des trois principaux opérateurs du pays – Bharti Airtel et Vodafone. La défection de l'Inde est aussi celle d'un pays asiatique, un voisin immédiat de la Chine, avec qui elle partage 3 500 km de frontière. Les observateurs n'ont pas manqué de remarquer que l'exclusion de Huawei survenait à un moment de tension exacerbée entre Pékin et New Delhi. En juin, des combats violents ont opposé des unités militaires indiennes et chinoises à la frontière tibétaine et fait des dizaines de morts côté indien. Plus que les considérations techniques ou économiques qui tarabustent les opérateurs européens, n'est-ce pas la feuille de route politique du gouvernement chinois – traduite localement par le positionnement de ses troupes dans les montagnes himalayennes – qui a décidé New Delhi à sanctionner Huawei ? À bien y penser d'ailleurs, peut-être que la chute des

dominos européens est également liée à un changement de regard porté sur la Chine de Xi Jinping. Car en à peine un an, les occasions n'ont pas manqué.

---

*1. Torture par simulacre de noyade.

*2. Voir chap. III, p. 77.

*3. Voir chap. VI, p. 180.

CHAPITRE VIII

La question idéologique

En dépit des actions judiciaires intentées contre Huawei pour des motifs divers et souvent anciens, il apparaît toujours plus clairement que son principal crime est d'être chinois. Face au gouvernement autoritaire – et qui se durcit – de Xi Jinping, les États-Unis assument mener un combat idéologique. Dès lors, que peut faire le champion chinois des télécoms ? Encaisser les coups et tenter de survivre.

Crise de confiance

Le 13 juin 2019, le *Globe and Mail* publie un article qui va secouer la classe politique canadienne. Le quotidien de référence du pays titre : « Chrétien propose d'annuler le dossier d'extradition de Meng pour dégeler les relations avec la Chine[1] ». Les journalistes ont eu vent de discussions tenues en Chine par l'ancien Premier ministre Jean Chrétien. Ce redoutable animal politique, qui a dirigé le pays pendant dix ans et n'a pas hésité à s'opposer à la guerre en Irak, à la fureur de George W. Bush, a été l'artisan historique des bonnes relations sino-canadiennes. Libéral, comme Justin Trudeau, il a gardé

des contacts à Pékin. Et il se verrait bien en médiateur pour sortir son pays de la crise où l'ont précipité les États-Unis en demandant l'arrestation de la directrice financière de Huawei à Vancouver. Comme d'autres, il fait valoir que l'extradition est un processus aussi politique que judiciaire et qu'il ne tient qu'à la ministre de la Justice d'y mettre un terme. Sa suggestion sera aussitôt rejetée par l'intéressée, arguant qu'il s'agirait là d'un « dangereux précédent ».

Ce que ne dit pas la ministre canadienne, c'est que le moment est très mal choisi. En effet, dans un télescopage dont l'histoire a le secret, les forces de sécurité chinoises viennent d'envahir les rues de Hong Kong. Depuis un mois, les habitants de la riche mégalopole rétrocédée à la Chine par la Couronne britannique en 1997 manifestent par centaines de milliers, si ce n'est par millions. Ils dénoncent le non-respect de la parole donnée douze ans plus tôt par la Chine de laisser son autonomie au petit territoire. Le déclencheur de la crise a été une loi d'extradition entre Hong Kong et le continent – ce qui ne manque pas de sel quand on se rappelle qu'au même moment, Meng Wanzhou se démène pour échapper à un dispositif similaire sur l'autre rive du Pacifique. Les manifestants de Hong Kong réclament le retrait du texte, le départ de la cheffe de l'exécutif hongkongais Carrie Lam – accusée d'être un pantin placé par la Chine –, et le suffrage universel. Pékin a d'abord fait la sourde oreille, puis amassé des troupes à Shenzhen, en guise d'avertissement. Après des semaines de cortèges monstres, le gouvernement chinois en a assez. Il est déterminé à faire plier la petite cité rebelle, quoi qu'il en coûte à son image internationale. Le 12 juin 2019, la répression s'engage et les images de violences font le tour du monde. Entre la Chine et le Royaume-Uni – l'ancienne puissance coloniale restée très liée à Hong Kong –, le torchon brûle. Boris Johnson, pressenti pour devenir incessamment Premier ministre, affirme son soutien total aux

manifestants, s'attirant les foudres de Pékin. Bientôt, il offrira la citoyenneté britannique aux résidents de Hong Kong, provoquant un nouvel accès de fureur à Pékin. Mais il n'y a pas qu'à Londres que la violente reprise en main des autorités chinoises inquiète. Dans toutes les capitales occidentales, la crise de Hong Kong provoque un sursaut, une prise de conscience de la nature répressive du pouvoir chinois. Elle va inévitablement jouer en défaveur des grands groupes technologiques de Shenzhen.

L'été passé et Hong Kong maté, un autre dossier viendra ternir encore davantage l'image de Pékin en Occident. Le 25 novembre 2019, dix-sept grands médias internationaux – dont *Le Monde* en France – publient une série d'enquêtes, toutes tirées des « China Cables », un vaste ensemble de documents internes au PCC obtenu par le Consortium international des journalistes d'investigation (ICIJ)[2]. L'organisation à but non lucratif qui regroupe des centaines de reporters et travaille avec les plus grands titres internationaux, de la *BBC* à l'*Asahi Shimbun* en passant par *Haaretz*, le *New York Times* ou la *Süddeutsche Zeitung*, s'est fait connaître par des révélations sur les dessous de la finance mondiale. Deux ans plus tôt, son travail sur les « Panama papers » et les paradis fiscaux lui a valu le prix Pulitzer. Cette fois-ci, ce ne sont pas des magouilles comptables que les « China Cables » mettent à nu, mais un vaste réseau de centres d'internement secrets où la Chine de Xi Jinping détient au moins un million de personnes de la minorité musulmane ouïgoure. Dans ces camps, que Pékin décrit comme des « centres d'éducation et formation » pour lutter contre le séparatisme islamiste dans sa province du Xinjiang, l'endoctrinement idéologique est la règle, la torture, une option. Les condamnations internationales vont pleuvoir une nouvelle fois. Même l'ONU demande une enquête et un accès au Xinjiang. Rien n'y fait, les critiques glissent sur le pouvoir chinois qui

n'hésite pas à montrer les dents, invitant les chancelleries occidentales à ne pas se mêler des affaires internes du pays – qu'il s'agisse de Hong Kong ou du Xinjiang. Pour les groupes technologiques chinois, et pour Huawei en particulier, cette nouvelle mauvaise publicité est bien pire que la précédente, car leur rôle est pointé du doigt. Selon les documents obtenus par l'ICIJ, le contrôle total de la population au Xinjiang repose largement sur une infrastructure de surveillance high-tech qui scanne, fiche et note chaque citoyen. Quel rôle y joue Huawei, le champion national des télécoms, qui vend partout dans le monde son offre de « villes sûres » ? Quelques mois plus tôt, lors d'une audition très musclée au Parlement britannique, le directeur de la cybersécurité de Huawei, John Suffolk, déclarait que le groupe ne travaillait « qu'avec des tierces parties » au Xinjiang et n'était qu'un fournisseur parmi des centaines d'autres, avant d'esquiver de son mieux les attaques des députés sur la question des droits de l'homme[3]. Mais quelques jours après la sortie des « China Cables », un rapport de l'Aspi – le même think tank devant lequel le patron des cyber-espions australiens faisait son premier discours public un an plus tôt – s'attardait au contraire en longueur sur les contrats signés par Huawei dans la province depuis 2011 et sur le caractère central de ses technologies pour y assurer un contrôle social orwellien[4]. Une semaine après cette publication, Ren Zhengfei donnera sa position dans une interview aux journalistes canadiens du *Globe and Mail*. « Nous sommes comme un fabricant de camions, qui vend des camions à différents pays. Ce qui est transporté dépend du conducteur, pas de nous », se dédouane le patron, qui semble par ailleurs soutenir la politique de son gouvernement dans la province à majorité musulmane. « Qu'est-ce qui est meilleur pour la population, selon vous, la solution des États-Unis pour le Moyen-Orient ou la solution de la Chine pour le

Xinjiang ? Le Xinjiang s'est progressivement stabilisé ces dernières années et il n'y a pas eu de problèmes sociaux majeurs ou d'affaires criminelles là-bas. L'économie du Xinjiang est également en croissance. Si la richesse d'une société s'accroît et que sa distribution devient raisonnable, de nombreux conflits vont progressivement s'estomper[5]. »

La liberté est-elle un prix acceptable à payer, en échange du confort matériel et de la sécurité ? Ce n'est pas un débat strictement chinois. Les pays occidentaux, avec leur empilement de lois antiterroristes depuis vingt ans, ont leur lot d'accommodements avec les grands principes, au point de vendre parfois leurs propres systèmes de surveillance high-tech à des dictatures peu recommandables – les logiciels du français Amesys par exemple, fournis à la Libye du colonel Kadhafi ou à l'Égypte du maréchal Sissi[6]… Mais ces compromissions n'empêchent pas les démocraties occidentales de considérer les camps du Xinjiang comme une violation exceptionnelle des droits de l'homme, dont ils rendent responsable la Chine de Xi Jinping. L'irruption fin 2019 d'un nouveau coronavirus à Wuhan et les manœuvres de Pékin pour masquer la gravité de l'épidémie à ses débuts ne feront qu'accentuer leurs inquiétudes. Une crise de confiance est ouverte. Elle va coûter cher à Huawei. Le groupe pouvait se défendre contre des attaques sur le plan technologique ou économique. C'est bien plus difficile lorsque la bataille devient idéologique.

Un mystérieux comité syndical

Huawei a toujours prôné sa totale indépendance vis-à-vis du gouvernement et, derrière lui, du PCC. Selon ses dirigeants,

l'entreprise est privée, depuis ses débuts, et n'a jamais reçu d'instructions de Pékin. Il est notable que les trois autres « tigres » chinois des télécoms qui se faisaient les griffes dans les années 1990 – ZTE, Datang et Julong – avaient tous l'État au capital. Mais c'est Huawei, qui ne bénéficiait pas d'un tel soutien, qui a éclipsé tous ses pairs. « Quand on se trouve dans un pays étranger, les gens nous regardent comme des communistes à cause du contexte chinois et prennent le bâton pour nous frapper sur le dos, se désole Ren Zhengfei. En Chine, les gens prennent aussi le bâton pour nous frapper sur les fesses parce qu'on nous qualifie de capitalistes[7]. » En dehors de ses frontières, le procès en communisme intenté à Huawei repose parfois sur des arguments à la limite de la mauvaise foi. Il est par exemple fréquent d'entendre reprocher l'existence d'un comité du PCC à l'intérieur de l'entreprise. C'est un fait que le patron n'a aucun mal à expliquer, puisque toutes les entreprises en Chine doivent légalement disposer d'une telle structure – y compris, remarque-t-il malicieusement, les filiales locales de multinationales américaines comme IBM ou Coca-Cola. À l'en croire, ce comité politique n'intervient pas dans les décisions de l'entreprise. En plus d'animer la communauté en ligne Xinsheng, il n'est chargé que de « la morale et de l'intégrité des employés[8] ». La formule peut bien écorcher quelques oreilles occidentales, peu de gens ont émis l'hypothèse que ce comité du PCC, élu en interne comme dans toutes les entreprises chinoises, tire les ficelles du numéro 1 mondial des télécoms – même si plusieurs universitaires ont écrit que le secrétaire du parti au sein de l'entreprise, Zhou Daiqi, siégeait au conseil de surveillance[9].

Huawei a la partie plus difficile, en revanche, pour convaincre que sa structure capitalistique le met à l'abri de toute ingérence politique. « À qui appartient Huawei ? » La question est si brûlante qu'à partir de 2018, elle figure en première page des rapports annuels du

groupe. La réponse de Huawei est simple : l'entreprise appartient intégralement à ses employés et « aucune agence gouvernementale, ni aucune organisation extérieure ne détient des actions dans Huawei[10] ». L'entreprise n'est certes pas cotée en Bourse, mais la moitié de ses 200 000 salariés détient des « actions virtuelles », qui donnent droit au paiement annuel de dividendes et la possibilité de participer à des élections internes pour désigner un collège de 115 représentants, eux-mêmes chargés d'élire le conseil d'administration et le conseil de surveillance du groupe.

Cet actionnariat salarié relève pourtant d'un « mythe », selon Donald Clarke et Christopher Balding, deux chercheurs américains qui se sont attelés à le « réfuter une bonne fois pour toutes » au printemps 2019[11]. Sur 15 pages, les deux professeurs – respectivement de l'université George-Washington aux États-Unis et de l'université Fulbright au Vietnam – décortiquent la gouvernance de Huawei, en s'appuyant sur des données institutionnelles et sur la presse chinoise. Ils pointent le fait que Huawei est détenu à 100 % par une structure chapeau, Huawei Investment & Holding, qui n'a elle-même que deux actionnaires. Ren Zhengfei en détient 1 % et les 99 % restants appartiennent à un Comité syndical de Huawei Investment & Holding. L'opacité qui entoure cette structure incite les deux universitaires à la prudence, mais ils soulignent que si ce comité syndical fonctionne bien comme n'importe quel autre syndicat en Chine, il dépend légalement de l'ACFTU (All-China Federation of Trade Unions), elle-même contrôlée par le PCC. Sans parvenir à une conclusion sur la question de savoir qui possède réellement Huawei, les deux chercheurs assurent qu'il ne s'agit certainement pas des employés. « Ils n'ont aucun droit de contrôle, ni n'exercent de gouvernance sur aucune entité de Huawei. […] En somme, Huawei n'est ni détenu, ni gouverné par les employés », écrivent-ils. Tout au

plus sont-ils les bénéficiaires d'un programme d'intéressement aux résultats.

Immédiatement après la sortie du rapport, Huawei dénoncera ses conclusions « complètement infondées ». Et deux semaines plus tard, le groupe accueillera la plus grande délégation de journalistes internationaux jamais vue dans ses bureaux de Shenzhen. Pour tenter de mettre fin aux spéculations sur son actionnariat, Huawei lui ouvrira sa « Shareholding Room ». Cette pièce terne est logée dans un petit bâtiment flanqué d'un lac où nagent des cygnes noirs, au cœur du vaste campus du groupe. C'est ici qu'est conservé, sous vitre et sous clé, un imposant registre bleu, en dix volumes, qui contient, selon Huawei, le nom de chacun de ses 104 572 salariés actionnaires et le nombre de ses actions. En plus de dévoiler cet énorme recueil manuscrit – que Donald Clarke et Christopher Baldwin raillent sous l'appellation « registre Potemkine » –, Huawei précisera que le fameux comité syndical qui représente ses salariés actionnaires n'est qu'une manière de contourner la législation chinoise, qui limite à 200 le nombre d'actionnaires d'une société privée. Enregistré auprès du syndicat municipal de Shenzhen, il n'aurait pas d'autre véritable fonction… si ce n'est de superviser le club de basket et d'organiser les tournois de badminton ou de ping-pong[12].

Des « actions virtuelles » très efficaces

Quel que soit le rôle effectif du comité syndical, le système d'« actions virtuelles » de Huawei qu'il met en œuvre est, lui aussi, très particulier. Elles ne peuvent être détenues que par les employés de nationalité chinoise. En fonction de leur performance – et généralement pas avant trois années d'ancienneté –, ces salariés s'en

voient proposer un certain volume. Ces « actions virtuelles » ne sont pas gratuites, il leur faut les acheter, à un prix déterminé chaque année en fonction de la valeur estimée de l'entreprise rapportée au nombre d'actions. Une fois titulaires de ces actions, les salariés ne peuvent pas les vendre, les donner à des tiers, ni même à d'autres employés. Seul le comité syndical peut racheter les titres. Et lorsqu'un employé quitte Huawei, il lui est défendu de conserver ses actions, qu'il lui faut revendre au comité syndical. Seuls les retraités et les employés justifiant d'une grande ancienneté peuvent conserver leurs titres – sans en disposer librement pour autant.

Malgré ces contraintes, la formule rencontre un grand succès auprès des salariés éligibles, car elle peut s'avérer très lucrative. Le cours de l'« action virtuelle » est passé, selon le *South China Morning Post*, de 5,42 yuans en 2010 à 7,85 yuans en 2019[13]. Une jolie pirouette, sans compter que les dividendes peuvent aussi rapporter gros. À raison de 1,05 yuan par action en 2018, le rendement du dividende de l'action Huawei se classerait dans les meilleures performances mondiales. Le groupe reste très secret sur le sujet, mais il y aurait environ 20 milliards d'« actions virtuelles » en circulation, ce qui aurait permis de redistribuer 3,2 milliards de dollars en 2018 aux salariés éligibles – environ un tiers des profits du groupe –, le genre de répartition qui ferait sauter de joie bien des syndicalistes en Europe. Chez Huawei, pour la grande masse de salariés qui possèdent plusieurs dizaines de milliers d'actions, c'est un confortable complément de revenu.

C'est d'ailleurs l'origine même du système, selon Huawei. Ren Zhengfei n'avait pas les moyens de payer ses ingénieurs de généreux salaires aux débuts de l'entreprise. Les rémunérer en actions et en promesses de dividendes futurs était une alternative peu coûteuse. Les années passant, le programme s'est avéré un formidable atout

pour le groupe. Il lui permettait non seulement de lever des fonds directement auprès de ses salariés, mais aussi de les motiver financièrement – particulièrement les plus méritants. C'est devenu une composante fondamentale de la « culture loup ». L'entreprise demande des sacrifices conséquents à ses employés, mais elle le leur rend en monnaie sonnante et trébuchante. Mieux, elle rémunère ainsi une large partie de ses équipes – et non pas seulement quelques cadres dirigeants. Et la valeur de cette prime dépend largement des résultats à long terme de la compagnie, au contraire des systèmes de retraites chapeau et autres mécanismes qui récompensent couramment dans les entreprises cotées des dirigeants en dépit de décisions calamiteuses. Ces mérites de l'actionnariat salarié sonneront familièrement en Europe – et en France en particulier – où les gouvernants, de De Gaulle à Sarkozy, en ont longtemps fait un rempart à la toute-puissance des marchés. Ren Zhengfei fera lui-même ce parallèle avec le Vieux Continent, assurant que ce « capitalisme des employés », sans « multimilliardaire dans l'entreprise », pouvait être « un modèle pour la plupart des entreprises à l'avenir »[14].

Face aux incompréhensions extérieures, Huawei s'est néanmoins régulièrement posé la question d'entrer en Bourse et de « normaliser » son fonctionnement. Mais le groupe n'a jamais sauté le pas. Les inconvénients d'une telle option l'ont toujours emporté sur les avantages, dans l'esprit de ses dirigeants. Le groupe n'en a jamais éprouvé le besoin financier. Et il a toujours douté que cela suffise à rassurer des critiques enfermés dans leurs certitudes. « Ce débat n'a rien à voir avec la sécurité, car la cotation n'a pas levé les suspicions sur notre concurrent chinois ZTE. Cela n'a même rien à voir avec la transparence – sinon il n'y aurait pas eu d'affaire Enron[15] », expliquait dès 2013 aux *Échos* le président du conseil d'administration de

Huawei France, François Quentin. Les déboires de son concurrent de Shenzhen, dont le cours de l'action a plongé dans la foulée des sanctions américaines de 2018, ont raffermi cette conviction. En restant privé, Huawei est mieux à même de résister aux attaques du gouvernement américain, comme d'éventuels actionnaires « activistes » qui n'hésitent pas à dépecer les grands groupes pour mieux les valoriser sur les marchés.

D'autant plus qu'*a contrario*, son modèle original lui procure la liberté fondamentale de s'affranchir de l'œil inquisiteur des marchés, qui scrutent, trimestre après trimestre, les performances et les décisions des groupes cotés sous le seul prisme de la rentabilité immédiate. Avec cette pression, Huawei aurait-il pu faire ses choix d'investissement audacieux dans la recherche ? « Si Huawei était une entreprise publique, nous n'irions pas exercer nos activités dans des pays sous-développés et déchirés par la guerre, dans des régions touchées par le paludisme ou dans l'Himalaya, relève aussi Ren Zhengfei. Faire des affaires dans ces régions n'est pas rentable du tout[16]. » D'une certaine façon, il valide les craintes américaines que l'entreprise n'agisse pas que sur des motifs économiques et commerciaux. Mais le patron l'assume. Il travaille pour « le bien de l'humanité ».

Ces deux dernières années, l'opposition du fondateur de Huawei au modèle de la Bourse s'est durcie. À un journaliste allemand qui l'interroge au printemps 2019 sur une cotation de son groupe, il répond : « Pas avant 3 000 ans[17]. » Et, dans ses prises de parole, transparaît plus qu'un désintérêt, une défiance. « Wall Street gagne beaucoup d'argent alors que les scientifiques n'ont que très peu. C'est peut-être la raison pour laquelle les scientifiques préfèrent nous rejoindre[18] », explique-t-il à Bloomberg TV, peu de temps après avoir expliqué au magazine *Fortune* – autre emblème du monde des

affaires anglo-saxon – qu'« il y a très peu d'histoires de réussites des entreprises dans lesquelles le capital occupe une place primordiale. Le capital est avide. Quand il y a un intérêt immédiat, le capital l'arrache, et perd sa poursuite à long terme de l'idéal[19] ».

Cette profession de foi anticapitaliste se doublera, peu de temps après, d'une critique contre la démocratie dans les processus de décisions internes à l'entreprise. Depuis les débuts de Huawei, Ren Zhengfei dispose en effet d'un droit de veto sur les décisions du conseil d'administration. Alors qu'il avait longtemps été question de supprimer cette relique autocratique des débuts, Huawei a finalement décidé de la pérenniser et d'en faire un pouvoir transmissible, après que le patron aura cédé la main à un « comité d'élites » de sept membres. « Quand on a vu le Brexit, nous avons pensé qu'il ne fallait pas laisser un processus démocratique décider tout seul du sort de l'entreprise[20] », explique sérieusement Ren Zhengfei. L'argument est audible. Reste que, dans la bouche de Huawei, c'est une nouvelle prise de position que ses contempteurs ne manquent pas de qualifier de politique. Il faut néanmoins remarquer que, même dans les grandes entreprises technologiques américaines, les exemples ne sont pas rares où le fondateur conserve un pouvoir absolu de décision – souvent grâce à d'astucieux systèmes de « double classe » d'actions, permettant de vendre des titres avec des droits de vote amputés. Facebook en est l'archétype, puisque Mark Zuckerberg, avec seulement 14 % des actions, dispose de 58 % des droits de vote et demeure le maître absolu de son groupe, sans aucun réel contre-pouvoir. Facebook n'est-il pas, en ce sens, beaucoup moins démocratique dans son fonctionnement que Huawei – où le fondateur dispose certes d'un droit de veto, mais dont il assure n'avoir jamais usé ?

Des critiques politiques

Les attaques contre Huawei se heurtent au même écueil. Si le groupe ne s'inscrit pas dans les canons occidentaux à bien des égards, nul n'a jamais apporté les preuves de ses prétendus comportements répréhensibles. Et c'est à juste titre que le groupe de Shenzhen dénonce un procès d'intention. Car c'est bien ce dont il s'agit. Fin janvier 2020, Robert Strayer et un collègue du Département de la justice, venu l'assister dans sa tournée d'avertissement sur la 5G, ne s'en cachent même pas. Face aux journalistes réunis à l'ambassade américaine à Paris, ils affirment le plus simplement du monde ne pas avoir besoin d'un *smoking gun* – le pistolet encore fumant qui signe le crime et constitue la preuve irréfutable de la culpabilité d'un suspect – pour dénoncer Huawei. « Si vous attendez un *smoking gun*, vous pouvez finir par vous faire tirer dessus, balaient les envoyés de Washington. C'est pour cela qu'il s'agit d'une question, plus vaste, de confiance. Et non de savoir si, oui ou non, ils ont déjà fait telle ou telle chose[21]. »

La phrase a le mérite de la clarté. La présomption d'innocence n'a pas lieu de s'appliquer. Et, pour l'administration américaine, cela ne tient pas tant au fonctionnement de Huawei qu'à la nature du système politique chinois. Un des arguments qui revient en boucle est celui selon lequel, quand bien même Huawei ne voudrait pas faire les quatre volontés de Pékin, la législation chinoise le lui impose. En 2017, la Chine a en effet voté une « loi sur le renseignement national », dont les termes de l'article 7 sont sans appel : « Toutes les organisations et citoyens doivent soutenir, coopérer et collaborer au travail du renseignement national et garder secrètes les opérations de renseignement national dont ils ont connaissance. L'État protégera les organisations et les citoyens qui soutiennent, coopèrent et collaborent

au travail du renseignement national. » Les Américains y voient la preuve que Huawei serait obligé de s'exécuter si Pékin lui demandait d'utiliser ses produits comme chevaux de Troie pour espionner ou saboter des infrastructures à l'étranger.

Le groupe chinois, lui, le nie farouchement. Dans une section appelée « Mythbusters » (« Briseur de mythes ») de son site institutionnel européen, l'entreprise tente de répondre méthodiquement à tout ce qu'elle considère comme des allégations mensongères à son encontre. L'un des cinq « mythes » est précisément l'assujettissement de Huawei à la loi chinoise sur le renseignement national. Le groupe assure que le texte « n'a aucune légitimité hors de Chine » et que des garde-fous existent dans le document. De fait, l'article 8 précise que le renseignement doit être mené « dans le cadre de la loi, en respectant et protégeant les droits de l'homme et en sauvegardant les droits et intérêts légitimes des personnes et organisations ». Pour que seule son analyse juridique ne fasse pas foi, Huawei renvoie au commentaire très officiel de Yang Jiechi. En février 2019, ce membre du Bureau politique du PCC a saisi la tribune de la prestigieuse Conférence de Munich sur la sécurité pour affirmer publiquement que « la loi chinoise n'exige pas des entreprises qu'elles installent des *backdoors* ou recueillent des renseignements ». Le groupe assure aussi à longueur d'interviews qu'il n'a jamais reçu une telle demande en trente ans d'existence et qu'il refuserait de s'y plier le cas échéant. Ren Zhengfei martèle qu'il s'y opposerait personnellement, quitte à aller derrière les barreaux. « Même si j'allais en prison, les conditions ne seraient pas aussi dures que dans d'autres cellules, plaisante le patron. De plus, tous les dîners y sont gratuits, donc ce n'est pas un problème pour moi, et je ne m'en fais pas du tout[22]. »

Malgré cet apparent détachement, les critiques du système chinois dans son ensemble sont bien difficiles à contrer pour Huawei. Et elles sont de moins en moins voilées. Quelques mois après avoir placé le groupe sur la liste noire des États-Unis, un haut responsable du Département d'État le reconnaît ouvertement lors d'une conférence sur « l'action multilatérale sur les technologies sensibles[23] » : « Le défi que présentent les géants technologiques chinois comme Huawei n'est pas, avant toute chose, un problème particulièrement "technique", même s'il a naturellement des aspects techniques importants. Fondamentalement, c'est un défi politique et géopolitique. » En 1992, le conseiller politique de Bill Clinton, James Carville, avait affiché dans son bureau le célèbre message « *It's the economy, stupid !* » (« C'est l'économie, idiot ! ») pour souligner la priorité absolue de la campagne. Un quart de siècle plus tard, les fonctionnaires américains pourraient adapter la formule et l'épingler aux murs : « *It's the ideology, stupid !* »

Quand ils effectuent leurs tournées européennes, les diplomates du Département d'État le rappellent aux autorités, aux opérateurs télécoms ou à la presse. « Ce que la Chine considère comme des motifs de sécurité nationale est bien plus large que dans les démocraties occidentales », répètent-ils. Certes, les États-Unis, comme les pays européens, mènent des opérations d'espionnage, mais « il ne s'agit pas de réprimer les oppositions politiques ou les minorités ethniques et religieuses, d'intimider les personnes qui dénoncent le régime ou même de pratiquer l'espionnage industriel […]. En Chine, c'est le cas. Et cela dérive du fait qu'il s'agit d'un État léniniste à parti unique ». Pour les diplomates américains, c'est une question systémique. Il y a bien des dérapages en Occident, mais ils sont limités par nombre de garde-fous, tels que des partis d'opposition, une presse libre, des tribunaux indépendants, une transparence

générale du gouvernement… « Rien de tout cela ne s'applique en Chine »[24], plaide le Département d'État.

Ironiquement, c'est une affaire qui a plus qu'embarrassé les autorités américaines qui leur sert désormais de passeport de vertu : celle qui a vu, début 2016, Apple s'opposer frontalement, et jusque devant les tribunaux, au ministère de la Justice. Le FBI exigeait alors de la firme à la pomme qu'elle déverrouille l'iPhone de Syed Farook, l'un des deux terroristes se réclamant de l'État islamique responsable de la mort de quatorze personnes dans une fusillade à San Bernardino, près de Los Angeles, en décembre 2015. Pour les besoins de l'enquête et de la lutte antiterroriste, la justice réclamait à Apple une *backdoor* dans ses téléphones. Sa crainte était que les données ne soient effacées automatiquement après la saisie de dix mauvais mots de passe, et la juge californienne Sheri Pym demandait l'« assistance technique raisonnable » d'Apple. Le patron de l'entreprise, Tim Cook, n'avait pas eu de mots assez durs pour dénoncer aussitôt un « abus de pouvoir » aux implications « effrayantes » et expliqué qu'« entre de mauvaises mains, ce logiciel, qui n'existe pas, pourrait déverrouiller n'importe quel iPhone. Même si nous pensons que les intentions du FBI sont bonnes, le gouvernement aurait tort de nous forcer à créer une porte dérobée pour pénétrer les téléphones[25] ». Quelques semaines plus tard, le combat judiciaire prenait fin. Le FBI avait réussi à accéder à l'iPhone de Syed Farook sans l'aide d'Apple. Cette issue scabreuse n'est pas ce que met en avant le Département d'État, quatre ans plus tard, mais bien le fait qu'Apple ait eu la possibilité d'attaquer son gouvernement. « Vous ne trouverez pas un seul exemple d'une entreprise chinoise qui ait assigné le gouvernement chinois en justice parce qu'elle pensait que le gouvernement avait fait une demande injustifiée de coopération sur des questions de sécurité ou de renseignement,

assure un porte-parole du Département d'État. Aux États-Unis, ce genre de dossiers remplit plusieurs étagères[26]. »

Dès lors, faut-il confier son réseau 5G – celui qui pilotera les usines, les véhicules, les villes de demain – à une entreprise qui ne s'inscrit pas dans le cadre démocratique et libéral occidental ? Pour les États-Unis, la réponse est non. Et tous les moyens sont bons pour le faire comprendre. Le Département d'État a même tourné un petit clip vidéo intitulé « Whose 5G can you trust ? » (« À la 5G de qui pouvez-vous faire confiance ? »), dans lequel il appelle à boycotter Huawei qui, non content de « violer les sanctions pour soutenir des régimes oppressifs comme celui de l'Iran » et de « voler de manière répétée la propriété intellectuelle », est tenu d'« obéir secrètement et de fournir des renseignements au Parti communiste chinois ». Le tout sur des images de mains s'échangeant furtivement des papiers ou des machines comptant des liasses de billets. La réalisation manque de subtilité, mais le message est clair. Dans le même registre kitsch, le téléfilm diffusé au Canada à l'automne 2019 sous le titre *Les Griffes du dragon rouge* est encore plus étonnant. L'intrigue de cette fiction de 54 minutes est « inspirée de faits réels », puisqu'il y est question de l'arrestation à Vancouver de la directrice financière et fille du fondateur du géant chinois Huashing, qui va provoquer l'enquête d'une intrépide journaliste et les représailles impitoyables de Pékin. Plus que les sous-entendus du scénario ou les performances des acteurs, c'est le nom du producteur qui retient l'attention. Il s'agit de Steve Bannon, le sulfureux ex-conseiller de Donald Trump, qui qualifie Huawei de « plus grave menace sur la sécurité nationale que nous [les Américains] ayons jamais affronté ».

Survivre, survivre, survivre

« Le plus fameux slogan de notre entreprise est : Survivre, survivre, il faut survivre », scande Ren Zhengfei. Le patron sait de longue date qu'un conflit ouvert avec les États-Unis est inéluctable. De son propre aveu, il a juste été surpris par son timing. « À cause de l'arrestation de Meng Wanzhou, le détonateur a été déclenché à l'avance[27] » – environ deux ans plus tôt qu'escompté, explique-t-il fin mai 2019 à la presse chinoise. L'effet des sanctions américaines commence à se faire sentir dès 2019. La croissance des revenus ralentit, affichant 19 % sur l'année contre près de 20 % un an plus tôt. Huawei estime à 12 milliards de dollars les recettes qui se sont envolées. Et le groupe sait qu'il a mangé son pain blanc. En 2019, nombre de ses téléphones haut de gamme en boutique étaient encore équipés de la suite applicative de Google. Le pire est à venir. D'ailleurs, la page de garde du rapport annuel 2019 n'est plus ornée de simples lignes de couleur, mais d'une image de phare dans la tempête. Dans un message de bonne année envoyé début 2020 à tous les employés du groupe, le vice-président tournant Eric Xu ne le cache pas : « Ce sera une année difficile » et « la survie sera notre première priorité », écrit-il, avant d'expliquer la nécessité de se séparer de 10 % des managers les moins efficaces et de réduire ou fusionner les équipes[28]. Ren Zhengfei peut bien se féliciter publiquement que la crise assainisse et soude le groupe, les voyants passent progressivement du vert à l'orange. Sur les neuf premiers mois de 2020, la croissance de Huawei n'atteint plus que 10 %. Sur le troisième trimestre, moins de 4 %. Le groupe cède des actifs : sa filiale de câbles sous-marins mi-2019 et, surtout, sa deuxième marque de smartphones, Honor, à l'automne 2020. Celle-ci représentait plus d'un quart des ventes de téléphones du groupe. Le consortium d'acteurs chinois qui a mis la main sur cette pépite n'a pas communiqué la somme payée, mais elle devait être rondelette. Pour

le géant des télécoms, l'idée n'est pas tant de récupérer du cash que de permettre à ces activités de prospérer hors de son giron. Sans l'étiquette « Huawei », peut-être Washington les laissera-t-il tranquilles…

Le groupe n'a pas peur des mesures chocs. Pour sortir de la nasse, Ren Zhengfei fait à l'automne 2019 un geste inouï. Le fondateur de Huawei propose de vendre sous licence sa technologie 5G à des groupes tiers. « Nous sommes prêts à accorder une licence exclusive à une entreprise américaine, étant donné que les États-Unis n'ont pas de technologie 5G, contrairement à l'Europe, au Japon et à la Corée du Sud », assure le septuagénaire à la chaîne CNBC, ajoutant que seraient inclus dans cet accord le code source, les logiciels et peut-être même le design des puces de Huawei. Le patron se dit « certain de gagner la course à la 5G » et ouvert à laisser les États-Unis accéder à toutes ses trouvailles, ce qui permettrait à Huawei de « financer encore plus d'innovations ». Mais aucun prix ne sera jamais communiqué, et l'hypothèse d'une telle sortie par le haut est vite oubliée.

Pour ne pas laisser la situation lui échapper, Huawei mise aussi, plus que jamais, sur sa diplomatie du portefeuille. À Paris, rendez-vous est par exemple donné à la presse un jeudi matin de février 2020 à l'hôtel Shangri-La. Liang Hua, le président et discret numéro 2 de Huawei, a fait le déplacement dans la capitale française. Il a une annonce d'importance à faire. Huawei va construire sa première usine hors de Chine et a retenu l'Hexagone pour l'implanter. Le lieu reste à déterminer, mais l'Alsace tiendrait la corde. « La première phase de cet investissement représente 200 millions d'euros, entre le terrain, les bâtiments et les équipements. À la clé, il y aura la création de 500 emplois directs », assure le dirigeant, devant une grosse dizaine de journalistes. Officiellement, le gouvernement se

félicite chaudement de ce choix, mais aucun représentant de l'exécutif ne s'est déplacé. Selon une source ministérielle, Bercy voit dans l'annonce « un énorme coup de pression[29] » alors que les modalités d'application de la loi « anti-Huawei » ne sont pas encore connues.

Un autre signe fort montre que Huawei a conscience de la gravité de la situation. Pour la première fois, le groupe chinois riposte en justice et attaque le gouvernement américain en 2019. Un cap est franchi. Huawei avait toujours déploré officiellement les attaques de l'administration et du Congrès, mais il n'avait jamais poussé les portes d'un tribunal pour s'en plaindre – sans doute préoccupé par la mauvaise publicité que cela n'aurait pas manqué de lui valoir et soucieux de se ménager la possibilité d'accéder un jour au marché américain. Avant même que l'entreprise ne soit placée sur la liste noire du Département du commerce, Huawei dégaine une première plainte en mars 2019 et demande à une cour fédérale du Texas de déclarer anticonstitutionnelle la loi qui empêche les administrations américaines et leurs sous-traitants de se fournir chez Huawei ou ZTE, pour des motifs de sécurité nationale. Dix-huit mois plus tard, dans un long jugement de 57 pages, le groupe de Shenzhen sera sèchement débouté. Croyait-il en ses chances ? Ou était-ce une question de principe ? Alors que ses marchés exports – et notamment l'Europe – sont pour la première fois sérieusement menacés, il est vital de défendre la réputation du groupe et de porter un contre-discours haut et fort devant les tribunaux et à coups de conférences de presse monstres. En décembre 2019, le groupe réitérera la manœuvre, en attaquant cette fois la décision du régulateur américain de priver de fonds fédéraux les petits opérateurs ruraux qui seraient équipés d'antennes chinoises, toujours au motif de préserver la sécurité nationale. Astucieusement, il se fait le défenseur des

marginalisés de la connectivité. « Des opérateurs de toute l'Amérique rurale, dans des petites villes du Montana, du Kentucky et des fermes du Wyoming choisissent de travailler avec Huawei parce qu'ils respectent la qualité et l'intégrité de nos équipements[30] », déclare le directeur juridique de Huawei, appelant le régulateur à ne pas mettre un terme à l'effort commun pour connecter ces communautés.

L'offensive ne se limite pas à l'administration américaine. Les foudres juridiques de Huawei s'abattent au même moment en France sur une journaliste de France 5, la société de production de son émission *C à vous* et l'une de ses invitées, la chercheuse française Valérie Niquet, responsable du pôle Asie à la fondation pour la recherche stratégique. Au cours de l'émission du 7 février 2019, intitulée *Huawei : qui a peur du géant chinois ?*, Valérie Niquet répond sans ambiguïté à la question de l'animatrice de la table ronde « Qui dirige Huawei ? » : « Il n'y a pas d'entreprise vraiment capitalistique au sens où on l'entend en Chine. Et dans chaque entreprise chinoise ou étrangère, il y a un comité du parti communiste qui fait partie de la direction. » Huawei réagira avec trois plaintes pour diffamation publique. Devant le tollé médiatique, après que la publication spécialisée *La Lettre A* a révélé l'existence de la procédure, le groupe précisera tout de même ne viser que « les auteurs des propos diffusés » et non les médias, ajoutant que « Huawei respecte leur indépendance et la liberté de la presse ». L'effet désastreux en termes d'image ne dissuadera pas le groupe d'intenter d'autres actions en justice, notamment en Suède pour contester son exclusion du marché de la 5G, sans succès.

La bataille de l'opinion

En plus de contre-attaquer en justice, le colosse chinois tente de reprendre la main dans l'opinion. L'année 2019 voit ainsi l'orchestration d'une opération de communication d'une ampleur rare. Selon le rapport annuel du groupe, pas moins de 4 500 journalistes, 3 000 chercheurs et experts, ainsi que plus de 1 000 délégations gouvernementales sont reçus au siège de Shenzhen. Plus de 300 personnes de 20 pays différents ont eu accès à la Shareholding Room où sont conservés les registres d'actionnaires de la société. Partout dans le monde, le groupe s'accroche. Lorsque la Nouvelle-Zélande interdit à son principal opérateur de s'équiper d'antennes chinoises pour la 5G, le groupe de Shenzhen se paie des pages de publicité dans les grands quotidiens du pays et des panneaux d'affichage géants dans les rues de Wellington proclamant : « La 5G sans Huawei, c'est comme le rugby sans la Nouvelle-Zélande[31]. » Au pays des All-Blacks, le slogan accrocheur déclenche la controverse chez les politiques et quelques détournements moqueurs des internautes kiwis, comme : « La 5G sans Huawei, c'est comme le Xinjiang sans surveillance. » Ce qui ne dissuade pas le groupe de poursuivre sa campagne. En Europe, il multiplie aussi les prises de parole. « On ne peut pas laisser dire tout et n'importe quoi sur Huawei », s'agace Weiliang Shi, le patron de la filiale française dans *Les Échos* le 18 février 2019, promettant de continuer à investir et à embaucher dans l'Hexagone.

Dix jours plus tôt, c'est au 82 rue d'Arlon à Bruxelles, à cinq minutes à pied du Parlement européen, que Huawei a donné rendez-vous au gratin des institutions. Ce soir-là, l'entrée du Concert Noble, un bâtiment gris de six étages aux hautes fenêtres cerclées de métal, est éclairée par de puissants spots. Un gigantesque tapis rouge dessine comme une langue qui parcourt le hall et deux volées de marches pour arriver jusqu'à la chaussée. Un projecteur affiche le

logo et le nom « Huawei » en plein milieu. À l'intérieur, des salles somptueuses à la décoration Louis XVI s'enchaînent jusqu'à l'imposante salle de bal de 400 m^2 et 15 m de hauteur de plafond. La pièce a vu passer le shah d'Iran, Lord Mountbatten, mais aussi un *Offizierskasino* nazi pendant la guerre. Début 2019, c'est l'écrin qu'a choisi le représentant de Huawei auprès de l'Union européenne, Abraham Liu, pour livrer un message musclé. Entre le récital de piano et un concert de jazz, l'ancien responsable de Huawei au Congo puis en Malaisie monte au pupitre pour redire l'importance de la cybersécurité pour le groupe. « Récemment Huawei a fait l'objet d'attaques constantes de certains pays et hommes politiques. Nous sommes choqués et parfois amusés par ces allégations dépourvues de sens et de fondement », explique le cadre en costume gris, avant de s'en prendre directement à l'ambassadeur américain auprès de l'Union européenne. « Hier, M. Sondland a dit que quelqu'un à Pékin pouvait faire sortir une voiture de la route à distance sur le réseau 5G et tuer la personne à l'intérieur. C'est une insulte à l'intelligence des gens, sans même parler des experts technologiques à travers l'Europe[32]. » Pour une fois, la riposte est aussi frontale que les attaques américaines.

Ren Zhengfei lui-même, qui s'était tenu résolument éloigné des médias pendant trois décennies, multiplie les entretiens. De janvier 2019 à mars 2020, huit recueils des interviews du fondateur sont publiés sous le titre *Dans ses propres mots*. Le premier exemplaire, un pavé de 113 pages, s'ouvre sur trois photos. Les deux premières sont prises par des employés de Huawei, au cours de missions d'installations difficiles – dans la jungle colombienne ou dans la boue indonésienne. La troisième est celle d'un avion soviétique de la Seconde Guerre mondiale, un Iliouchine Il-2, criblé d'impacts de balles et visiblement mal en point. La légende indique

qu'il continue à voler et parvient à regagner l'aéroport malgré ces dégâts effrayants et ajoute : « Les blessures forgent l'esprit et le corps d'un individu. Jamais dans l'histoire de l'humanité la vie des héros n'a été facile. » Le groupe chinois en fait un symbole de sa résilience. Peu importe qu'une enquête du site britannique *The Register* assure qu'il s'agit en réalité d'une capture d'écran du jeu vidéo *Il-2 Sturmovik : Battle of Stalingrad*[33]. Ren Zhengfei a lui-même trouvé l'image en ligne et l'a partagée en interne car elle lui faisait « penser à la situation de [leur] entreprise ». Le patron file à l'envi la métaphore aéronautique. « La question qui vous préoccupe est de savoir si le moteur de l'avion a été touché, n'est-ce pas ? demande-t-il à l'agence de presse chinoise Xinhua en mai 2019. Je vous dis que c'est simplement une partie marginale de l'aile qui est probablement atteinte, mais pour la partie cruciale, nous maîtrisons et nous prenons de l'avance sur le reste du monde[34]. » Au printemps 2020, lors de son sommet annuel en direction des analystes, la firme utilisera encore une fois l'image de l'Iliouchine amoché, projetée sur un écran géant avec la phrase : « Quand avancer devient dur, les durs continuent d'avancer. » Le message a le mérite d'être clair.

En dépit de cette campagne de communication dramatique, l'ambiance reste bonne au siège de Shenzhen, selon les nombreux visiteurs qui se succèdent dans les locaux du groupe. Dans les cafétérias du campus, le correspondant en Chine des *Échos*, Frédéric Schaeffer, rapporte que le café est servi dans des gobelets sur lesquels une image de phare a été imprimée avec le message « Le phare guette le retour rapide de Meng Wanzhou », mais c'est l'un des rares signes apparents de la crise. Au contraire, en mai 2019, alors que l'entreprise vient d'être placée sur la liste noire américaine, la cohésion interne paraît renforcée. Une lettre publique intitulée « Nous, les gens de Huawei » fait un tabac sur les réseaux sociaux en

Chine, après que le compte officiel de la communauté interne Xinsheng l'a publiée sur son compte Weibo – le Twitter chinois. Telle que le raconte le grand quotidien anglophone *China Daily*[35], il s'agit d'une succession de courts témoignages d'employés racontant comment les sanctions ont changé leur quotidien. L'un assure que sa petite amie ne lui reproche plus de faire trop d'heures supplémentaires, un autre déclare que les pauses à la cantine sont plus courtes tant les salariés ont hâte de retourner travailler… Le succès de la lettre – lue, partagée et commentée des centaines de millions de fois en Chine – témoigne du soutien de la population chinoise à son champion injustement attaqué. Cet attachement n'est pas que virtuel, car il se traduit en boutique. En achetant un smartphone Huawei, les consommateurs chinois font coup double. Ils acquièrent un excellent appareil et font un geste patriotique. Les résultats du groupe de Shenzhen montrent l'ampleur du phénomène. En 2019, la hausse des ventes en Chine (+ 36 %) assure à elle seule la totalité de la croissance annuelle. Le marché intérieur, qui ne représentait que la moitié de l'activité en 2017 ou en 2018, approche en 2019 des 60 %.

Ce patriotisme économique a un inconvénient. Il aurait vite fait de flirter avec la propagande, ce qui pourrait se retourner contre Huawei. Début 2019, une vidéo virale intitulée « Huawei Beauty » et partagée par le quotidien nationaliste *Global Times* montre par exemple un groupe de petits enfants effectuant une chorégraphie et chantant des paroles telles que : « Nous aimons notre pays, nous aimons notre marque locale Huawei », ou encore : « Les puces fabriquées en Chine sont les plus précieuses[36]. » Ren Zhengfei, lui, se méfie de ces discours trop ouvertement patriotiques. « Choisir ou non les produits Huawei n'est pas synonyme d'aimer son pays ou pas. […] Jamais on n'a affiché la phrase "Nous battre pour la gloire de notre

pays” dans nos pubs[37] », insiste-t-il auprès d’un journaliste du magazine chinois *Caijing* en mai 2019. Le patron reconnaît que des slogans de ce type ont émaillé certains rassemblements internes, mais assure avoir immédiatement donné des consignes pour l’empêcher. S’il estime normal que son gouvernement le soutienne, dans la mesure où Huawei paie 20 milliards de dollars d’impôts en Chine chaque année, il ne souhaite pas entrer dans la spirale nationaliste.

Fondamentalement, Ren Zhengfei ne veut pas d’une fracture entre la Chine et l’Occident. Il est un fervent défenseur de la mondialisation et du libre-échange qui lui a si bien réussi et dont il aimerait continuer à profiter en tant que leader technologique. C’est ce qui explique les nombreuses tentatives de Huawei de préserver un environnement pacifique. Cela n’empêche pas le groupe d’être réaliste sur la portée du conflit dont les engrenages sont solidement en place dès 2019. Dans la foulée du placement sur la liste noire américaine, le responsable de la communication du groupe le pronostique très lucidement : « Cela pourrait conduire au début de la fragmentation des standards et de l’écosystème technologique mondial[38]. » La suite des événements lui donnera raison. Mais s’il déplore le schisme naissant, Huawei ne se résout pas à en être la victime. Contraint de s’adapter aux nouvelles règles du jeu, le géant de Shenzhen dispose toujours de son avance technologique, de ses brevets, de son assise financière et du soutien de la Chine – premier marché télécoms au monde. Sa capacité de résistance n’est plus à prouver. Contraint par l’Occident de se replier sur lui-même, il va s’efforcer de sortir de la crise plus fort qu’il n’y est entré.

CHAPITRE IX

Le monde d'après

Loin de s'apaiser avec le temps, les divergences sino-américaines s'étendent. Elles ne concernent plus seulement les deux superpuissances, mais l'ensemble du monde. Et elles ne se cantonnent plus à la 5G, mais englobent la tech dans son ensemble. Comme au temps de la guerre froide, deux écosystèmes radicalement différents émergent de la crise. Les conséquences sont difficiles à prévoir, tant elles dépendent de la volonté des différents acteurs d'éviter un embrasement général.

Huawei double la mise

Mi-septembre 2020, l'exposition des nouveaux produits de Huawei à destination de la presse française est aussi léchée qu'à son habitude. Les derniers ordinateurs portables, smartphones, enceintes et autres écouteurs intelligents de la marque au lotus rouge – dans des coloris variés – sont présentés sur des pupitres répartis dans une salle du dernier étage du 50 avenue des Champs-Élysées. Sur la terrasse ensoleillée, Walter Ji, qui dirige la branche Smartphones du

groupe en Europe de l'Ouest, fait montre d'un optimisme à toute épreuve. « Les sanctions américaines nous rendent la vie difficile, mais on y voit aussi une énorme opportunité », explique-t-il tout de go, en montrant son tee-shirt sur lequel sont imprimées neuf lignes parallèles, sinuant pour former un « H » stylisé. Pour les initiés, ce nombre est une des clés de la confiance du groupe chinois dans l'avenir. Il fait référence à sa stratégie « 1 + 8 + N », dévoilée à l'été 2019, qui consiste à connecter au sein de l'écosystème de la marque 1 smartphone à 8 périphériques essentiels (TV, tablette, PC, écouteurs, auto, montre, lunettes et enceintes) et N objets intelligents (imprimantes, projecteurs, caméras, capteurs divers et variés…). Et l'arme secrète de Huawei pour s'imposer ainsi dans le moindre recoin de nos vies numériques s'appelle « Harmony ». Il s'agit d'un tout nouveau système d'exploitation – le logiciel central qui pilote un terminal informatique, tels Microsoft et MacOS pour les ordinateurs ou Android et iOS pour les smartphones. Huawei y travaille depuis des années.

Ren Zhengfei parle souvent des « roues de secours » que son groupe a mises au point pour parer à toute éventualité. Harmony OS est sans doute le plus important de ces projets. Développer un système d'exploitation est une tâche gigantesque. Ceux qui s'y sont cassé les dents sont nombreux, de Blackberry à Samsung. Même Microsoft, malgré des milliards investis dans Windows Mobile, a spectaculairement échoué à se faire une place aux côtés d'Apple et de Google dans les smartphones. Il n'est pas étonnant que Huawei ne se jette à l'eau que contraint et forcé par les sanctions américaines qui l'ont brutalement privé des logiciels de Google. Bien sûr, la marche est haute. Il faut convaincre les développeurs de rendre leurs applications compatibles, quand Android et iOS affichent chacun des millions d'apps dans leurs magasins respectifs. Pour y parvenir,

Huawei a mis 1,5 milliard de dollars sur la table à l'automne 2019. L'objectif affiché est de recruter 5 millions de développeurs pour son AppGallery, un magasin d'applications déjà disponible sur sa version maison d'Android et qui sera demain le portefeuille d'applications d'Harmony. En plus de ce soutien financier, Huawei ne manque pas d'arguments pour séduire les concepteurs d'applis. Il est le deuxième vendeur de smartphones au monde et écoule chaque année 240 millions d'appareils, de quoi leur fournir une très large base d'utilisateurs potentiels. Sans compter que, tandis qu'Apple et Google sont régulièrement pris à partie par des développeurs outrés de devoir payer une « taxe » de 30 % sur toutes les recettes générées dans leurs applications aux géants californiens, Huawei a promis de ne prendre qu'une commission de 15 %.

Un an plus tard, Huawei a déjà séduit 1,8 million de développeurs et assure proposer près de 100 000 applications, dont les plus populaires dans chacun de ses 170 pays d'activité. « Nous sommes désormais le troisième plus grand écosystème mobile au monde », se félicite Richard Yu, le président de la branche Grand public de Huawei, le 10 septembre 2020, en dévoilant sur le campus de Dongguan la dernière version de Harmony. Cinq jours plus tard, sur les toits de Paris, son délégué pour l'Europe de l'Ouest précise que l'ambition va bien au-delà de proposer la première alternative crédible à Android et iOS. Tout comme Microsoft n'a jamais réussi à adapter Windows pour le mobile, le groupe chinois est persuadé que les deux géants américains des OS pour smartphones ne sont pas les mieux placés pour s'imposer dans la nouvelle révolution des objets connectés, qui se profile avec la 5G. Huawei, lui, est parti d'une feuille blanche pour concevoir Harmony. « Notre OS s'adapte à toutes sortes d'appareils nativement », assure Walter Ji. Déjà disponible sur les téléviseurs et montres connectées de la marque au lotus, il doit

équiper des smartphones dès la mi-2021, mais aussi tablettes, voitures, caméras… Un OS pour les gouverner tous, tel est le projet Harmony. L'idée n'est pas neuve dans la tech. Apple cherche laborieusement à faire fusionner ses systèmes d'exploitation pour smartphones et pour ordinateurs ; Google a un projet similaire. Une telle intégration permet aux utilisateurs de passer sans effort d'un type d'appareil à un autre, en transférant par exemple leur profil et leurs préférences. Elle offre surtout aux développeurs la possibilité de travailler sur une seule application, qui est ensuite disponible sur toute une galaxie d'appareils. Ce rêve de technophile a échappé aux plus grands noms de la tech américaine. Huawei sera-t-il le premier à le concrétiser ? Si une entreprise au monde a les ressources pour le faire, c'est le groupe de Shenzhen. Il a dans ses coffres 53 milliards de dollars de cash, sans compter le soutien sans faille des grandes banques d'État chinoises, sa puissance de R&D est redoutable et il dispose, très prosaïquement, de centaines de millions d'appareils Huawei sur lesquels proposer instantanément sa solution à travers le monde. Pour ne rien laisser au hasard, le groupe a déjà annoncé qu'il comptait faire d'Harmony OS une plateforme open source, mise à disposition des autres constructeurs, sur le modèle d'Android, ce qui signifie que, si le logiciel de Huawei est à la hauteur des ambitions de ses concepteurs, ce pourrait bien être un raz-de-marée – chez les fabricants chinois de smartphones mais aussi chez tous les industriels mondiaux, de l'automobile aux volets roulants en passant par les compteurs électriques intelligents… C'est le paradoxe des sanctions américaines. En poussant Huawei à s'émanciper des technologies étrangères, elles vont peut-être précipiter ce qu'elles cherchaient à éviter : l'émergence d'une superpuissance technologique chinoise. À Shenzhen, cela fait un moment que l'on ne cache pas cette ambition. Semblant faire fi des nuages noirs dans le ciel, Ren Zhengfei a

expliqué dès le printemps 2019 qu'il allouerait 100 milliards de dollars à la R&D sur cinq ans, et verrait les revenus de Huawei passer de 100 milliards à 250 milliards[1].

La lutte pour les standards

Si Huawei garde confiance dans sa capacité à surmonter la crise, c'est aussi que le groupe connaît la place centrale qu'il occupe dans les télécoms. Les montants colossaux que le groupe a investis en R&D ont amené avec les années des découvertes de plus en plus nombreuses. Cette maestria est reconnue par toute l'industrie. Elle se traduit dans les organismes de normalisation – les lieux où sont décidées les caractéristiques techniques communes de toute technologie à vocation mondiale. C'est notamment le cas pour les réseaux mobiles. Pour ne pas avoir de problèmes de compatibilité – comme à l'époque de la 3G où un téléphone européen ne fonctionnait pas aux États-Unis et vice-versa, faute de choix similaires sur les deux rives de l'Atlantique –, les industriels essaient de tomber d'accord en amont sur les meilleures options techniques à privilégier. Un marché mondial unifié est meilleur pour les affaires. Pour la 3G, puis la 4G et la 5G, l'enceinte privilégiée pour cette harmonisation s'appelle le 3GPP (3rd Generation Partnership Project), conglomérat de sept organisations régionales de normalisation de la planète entière. Huawei y est très bien introduit. Un rapport du cabinet IPlytics[2] de janvier 2020 montre que, pour la 5G, Huawei a soumis à lui seul au 3GPP un cinquième de toutes les propositions faites par tous les acteurs. Avec 26 372 contributions, le groupe de Shenzhen détient non seulement le record absolu, mais aussi celui de la plus large part de contributions aux standards – ces inventions très

spécifiques qui constitueront des briques essentielles et incontournables d'une nouvelle norme. Huawei est tellement indispensable qu'en juin 2020, les États-Unis ont fait une entorse très inhabituelle à leur liste noire pour autoriser explicitement les groupes américains à échanger avec le groupe chinois sur les spécifications de la 5G[3].

Détenir ces brevets « essentiels » est un avantage économique énorme. Cela permet à Huawei de nouer facilement des accords croisés pour accéder aux brevets de ses concurrents. Ou de se faire payer de juteuses licences. Sur les marchés dont Huawei serait exclu, ses rivaux Nokia et Ericsson auraient beau installer leurs propres antennes, ils resteraient contraints d'utiliser les inventions « essentielles » du groupe chinois et n'auraient pas d'autre choix que de passer à la caisse. Huawei est aussi intraitable sur le sujet que n'importe quelle autre entreprise technologique. En 2020, le groupe a déjà porté plainte contre l'opérateur américain Verizon, accusé d'utiliser sans son accord une dizaine de ses brevets. Quelques mois plus tôt, avant que l'affaire ne soit portée devant la justice, la presse américaine assurait que le groupe chinois réclamait plus d'un milliard de dollars à Verizon au titre de sa propriété intellectuelle[4].

En plus de rapporter gros, être un faiseur de normes permet de pousser sa vision d'une technologie, les usages qu'on souhaite lui permettre, les limites qu'on aimerait lui fixer… C'est ainsi qu'un sujet scientifique – « Quelle est la meilleure solution technique ? » – devient politique – « Que souhaite-t-on faire avec ? » Le fonctionnement des organismes de normalisation les rend étanche aux considérations politiques. Leurs membres appartiennent tous à l'industrie. Divisés en une multiplicité de groupes de travail où chacun apporte ses propositions techniques, ils votent pour décider

lesquelles intégreront le futur standard sur des critères purement scientifiques.

Du moins en théorie. Car, au moins en une spectaculaire occasion, ces beaux principes n'ont pas tenu. En novembre 2016, des flopées d'ingénieurs du monde entier sont réunies pour un vote crucial du 3GPP dans les salons d'un palace de Reno, aux États-Unis[5]. Il s'agit d'entériner certaines spécifications des futurs réseaux 5G – et en particulier de décider quel type de codes de correction d'erreurs l'industrie adoptera, c'est-à-dire quels outils mathématiques avancés serviront à « nettoyer » les signaux radio pour limiter les bugs tout en conservant des débits ultrarapides. Alors que la victoire semblait acquise à une catégorie d'algorithmes poussés par l'Américain Qualcomm, un retournement inespéré voit la méthode concurrente développée par Huawei terminer *ex aequo* dans la dernière ligne droite. Et ce grâce au changement de pied de dernière minute du groupe chinois Lenovo, dont le patron ira jusqu'à s'excuser pour son soutien initial à Qualcomm, jugé non patriotique. Ces combines électorales d'arrière-cour paraissent obscures. Elles ont pourtant des conséquences énormes. Grâce au vote de son compatriote Lenovo, Huawei a pu intégrer au standard 5G ses algorithmes, les fameux *polar codes* sur lesquels travaillait depuis des années dans ses laboratoires d'Ottawa le professeur Wen Tong, recruté par le groupe chinois dans la foulée de la faillite de Nortel. Huawei, qui avait misé des millions de dollars sur ce pari un peu fou, s'est ainsi vu *in extremis* assurer un retour sur investissement grâce aux droits de licence que lui verseront tous les futurs utilisateurs de la 5G. Mais cette victoire a été acquise au prix d'un vote plus politique que scientifique…

Ce genre de mésaventure est rare, à en croire des spécialistes de la normalisation. Mais il inquiète. Certains observateurs craignent

que la Chine ne noyaute les organismes de standardisation pour pousser son agenda technologique national – un peu comme Pékin est ouvertement critiqué, depuis la crise du Covid, pour avoir mis en coupe réglée l'Organisation mondiale de la santé. Dans l'univers technologique, c'est l'Union internationale des télécommunications (UIT), une agence peu connue de l'ONU, qui suscite probablement le plus de craintes. Depuis la libéralisation des années 1980 et le repli des États face aux grandes entreprises privées dans les télécoms, l'UIT a certes perdu de son influence face à d'autres organismes de standardisation comme le 3GPP, mais elle reste par exemple chargée de l'harmonisation du spectre radioélectrique sur la planète, ou encore de la numérotation téléphonique mondiale. En 2014, l'élection d'un Chinois à la tête de l'UIT ne provoque pas de remous particuliers. Pourtant, « en regardant en arrière, le timing était presque parfait », explique Dominique Lazanski, ex-directrice des affaires publiques de la GSMA, l'association qui regroupe les opérateurs et équipementiers mobiles du monde entier, dans une tribune au magazine *Forbes*. « Alors que l'industrie mobile et le reste du monde se concentrent sur les standards 5G du 3GPP, la Chine utilise l'UIT pour pousser sa propre version nationale de la 5G qui […] autorise une tierce partie, comme le gouvernement, à valider l'accès des utilisateurs[6]. »

La critique fait écho à un projet, porté par Huawei auprès de l'UIT dès 2018, et baptisé « New IP ». Dans une présentation PowerPoint intitulée « Vers un nouvel Internet pour l'an 2030 et au-delà[7] », Richard Li – le patron de la recherche du groupe de Shenzhen aux États-Unis – en dessine les contours. Le constat initial est que le protocole internet ou « IP », un système d'adressage inventé il y a un demi-siècle où chaque terminal connecté au réseau possède un identifiant unique (l'adresse IP), est inadapté à des usages futuristes

comme les hologrammes, l'Internet tactile… Huawei juge la norme actuelle inefficace et pas assez sûre. En revoyant radicalement la façon d'écrire les adresses sur lesquelles reposent les échanges d'information sur la Toile, les ingénieurs de Shenzhen veulent ouvrir la porte à ces technologies révolutionnaires. Mais les critiques les soupçonnent de concocter, par la même occasion, une refonte d'Internet dans laquelle il serait bien plus facile qu'aujourd'hui de centraliser les flux dans les mains de l'État pour refuser certains usages ou utilisateurs. En clair, de tailler un Internet sur mesure pour la Chine ou d'autres régimes autoritaires. Selon le *Financial Times*[8], la proposition de New IP aurait d'ailleurs reçu le soutien de la Russie et de l'Arabie saoudite. La perspective d'un tel « standard » fait *a contrario* bondir les Occidentaux – notamment le Royaume-Uni, la Suède et les États-Unis. La crainte de ces pays démocratiques n'est pas tellement de devoir s'aligner sur New IP, mais plus qu'une telle hypothèse ne provoque, en réalité, un éclatement du réseau mondial.

Splinternet

L'hypothèse d'un grand schisme d'Internet a un nom. Avec leur génie des mots, les Anglo-Saxons parlent de « Splinternet », contraction de *split* (diviser) et *Internet*. Mais ni le terme ni la réalité d'un réseau fracturé ne datent en réalité de la crise sino-américaine autour de la 5G. Depuis les débuts du Web, l'expérience n'en est pas la même partout dans le monde, principalement en raison des mesures de censure – dont l'exemple chinois est sans doute le plus abouti. Derrière le Great Firewall des autorités de Pékin, la plupart des sites d'information occidentaux, mais aussi les principaux réseaux sociaux – dont Facebook – sont inaccessibles. Quant à Google, après

avoir vainement tenté de percer le marché chinois et de résister aux pressions de Pékin pour filtrer les résultats de recherche en Chine, le groupe a fini par jeter l'éponge il y a plus de dix ans – convaincu que les autorités chinoises avaient commandité une audacieuse attaque informatique sur ses serveurs, ayant abouti au piratage des boîtes e-mails d'opposants chinois et au vol de son précieux code source. Pour n'importe quel internaute qui a surfé de part et d'autre du Great Firewall, on peut déjà parler de « Splinternet ». Seulement la facture qui se profile aujourd'hui est d'une ampleur et d'une nature différentes.

Première différence notable, ce sont des contenus et services chinois qui commencent à être bannis de plusieurs endroits du monde, dans une sorte de mouvement symétrique à la censure historique de Pékin. En 2020, l'Inde a frappé très fort, interdisant en l'espace de quelques mois plus de 200 applications mobiles chinoises, pour des motifs de sécurité nationale. Parmi les victimes de cette offensive inédite, on compte la messagerie WeChat, le jeu vidéo PUBG – l'appli qui générait le plus de revenus de tout le pays –, ou encore le réseau social TikTok. Pour ce dernier, véritable phénomène de société chez les ados du monde entier, la perte de l'Inde est un coup dur. Avec 120 millions d'utilisateurs, il s'agissait de son principal marché à l'export. Quand, quelques semaines plus tard, Donald Trump lui barre la route des États-Unis – où 90 millions de teenagers étaient aussi accros à son système de partage de courtes vidéos –, c'est un coup de tonnerre. Le propriétaire de TikTok, le groupe chinois ByteDance, a 45 jours pour trouver un repreneur américain à ses activités aux États-Unis. Par la même occasion, Trump ferme la porte à WeChat et sous-entend qu'il pourrait prendre des mesures contre Alibaba.

Pourquoi une telle censure ? Lorsqu'en 2019, les autorités américaines avaient demandé au groupe chinois Kunlun de revendre GrindR, une appli de rencontres gay achetée en 2016, le problème était clairement exposé. Washington ne voulait pas qu'une entreprise étrangère, *a fortiori* chinoise, mette la main sur des informations sensibles de ses citoyens (préférences sexuelles, séropositivité…). Mais pour TikTok, dont les pastilles vidéo les plus remarquées de 2019 incluent un furet qui danse et un mélange explosif Coca-Cola/Mentos version XXL… où est la menace ? Vue de Chine, la manœuvre est une nouvelle attaque gratuite de l'Oncle Sam, jaloux du succès de TikTok, premier réseau social à contester sérieusement l'hégémonie de Facebook et d'Instagram, y compris aux États-Unis. Mais vu de Washington, peu importe la nature des données envoyées par les jeunes Américains sur des serveurs chinois. Le volume énorme d'informations transmises permet de connaître très finement leurs habitudes. Et éventuellement de les influencer, en se servant de la plateforme comme la Russie a utilisé Facebook pendant l'élection de 2016. Enfin, sans doute y a-t-il aussi, de la part des États-Unis, la volonté de brider le développement d'un champion du logiciel. Car les vidéos virales n'ont pas attendu TikTok pour pulluler. Ce qui a fait le succès planétaire de l'appli chinoise, c'est son algorithme de recommandation, qui repose sur l'apprentissage automatique – autrement dit l'intelligence artificielle (IA). Et Washington a une peur bleue de se faire doubler par la Chine sur cette technologie clé, comme il s'est fait prendre de vitesse pour la 5G.

Pour Eric Schmidt, l'ancien patron de Google, la confrontation avec Huawei a constitué pour les États-Unis « un moment Spoutnik[9] ». Le lancement du petit satellite en 1957 avait ébranlé Washington, qui ne pensait pas l'URSS capable d'une telle prouesse et avait rapidement musclé ses propres capacités spatiales. De même, la

5G a été pour l'Amérique un signal d'alarme, en ce qu'elle a révélé la capacité de la Chine, non plus à imiter, mais à innover sur des technologies de pointe. Ceux qui pensaient que le modèle autoritaire chinois ne permettrait pas le foisonnement créatif nécessaire avaient tort. Au contraire, la mobilisation de budgets publics colossaux, la possibilité de tester sur un marché domestique immense, protégé et moins contraint par les freins juridiques ou éthiques de l'Ouest, ont permis de prendre de l'avance sur des technologies critiques comme la 5G, l'IA, l'informatique quantique… Comme en 1957, les États-Unis ont été saisis par la perspective de se faire dépasser technologiquement. Et comme en 1957, ils ont réagi vivement. À l'automne 2019, plusieurs stars chinoises de la tech connaissent le même sort que Huawei et sont inscrites sur la liste noire du Département du commerce américain : les fabricants de caméras de surveillance Hikvision et Iflytek, mais aussi SenseTime et Megvii, deux cadors de l'IA, spécialisés notamment dans la reconnaissance faciale et valorisés respectivement 7,5 et 4 milliards de dollars. Le rôle de toutes ces sociétés dans la surveillance high-tech au Xinjiang est mis en avant. Mais c'est l'avantage stratégique qu'elles pourraient fournir à Pékin qui inquiète Washington, plus encore que le sort des Ouïghours.

Petit à petit, la guerre technologique s'étend. L'administration Trump présente à l'été 2020 un programme dénommé « Clean Network » (réseau propre), qui va bien au-delà de l'exclusion des fournisseurs chinois d'antennes 5G. Washington ne veut plus d'opérateurs télécoms chinois, ni de fournisseurs de cloud, de câbles sous-marins, d'applis mobile ou de magasins d'applis en lien avec Pékin. Ce ne sont pas que des mots. Google et Facebook doivent par exemple renoncer à poser un câble sous-marin. Prévu depuis 2016 pour relier Los Angeles à Hong Kong, il s'arrête finalement à Taïwan.

China Mobile s'est pour sa part vu refuser l'autorisation d'opérer des liaisons internationales depuis les États-Unis, tandis que les licences des deux autres grands opérateurs chinois sont contestées par le régulateur américain. Comme pour Huawei, les États-Unis ne veulent pas limiter leur offensive à leur territoire. Le Département d'État se targuait à l'été 2020 de pouvoir compter sur 30 « Clean Countries » (pays propres) et invitait tous ses alliés à effectuer leur grand ménage. Avec cette approche de cow-boy, Washington prend délibérément le risque de précipiter l'avènement d'un Splinternet bien plus radical qu'aujourd'hui. Au lieu de se concentrer sur les contenus, la fracture descendra cette fois jusque dans les couches basses de l'architecture du réseau, posant la question de la compatibilité à terme des deux sphères technologiques qui se mettent en place.

L'administration Trump ne s'en émeut pas. Au contraire, elle paraît déterminée à rendre le divorce franc et irréversible. Mi-novembre, alors que la victoire de Joe Biden est acquise, Donald Trump continue de prendre des mesures spectaculaires. Le président cherche à couper l'accès des entreprises chinoises aux marchés financiers américains. Cela passe d'abord par un décret interdisant aux Américains d'investir dans une liste d'entreprises jugées proches de l'armée chinoise : Huawei, China Mobile et China Telecom, mais aussi les groupes nucléaires CNNC et CGN, le constructeur aéronautique Avic, l'entreprise d'armement Norinco, certains groupes de construction… Quelques jours plus tard, c'est au tour du gendarme de la Bourse de faire un coup d'éclat de fin de mandat, en restreignant les conditions d'accès aux marchés américains des entreprises chinoises, avec une série de règles qui pourraient aboutir à un retrait de Wall Street pour plusieurs d'entre elles. Le timing de ces annonces peut surprendre. Elles sont très inhabituelles pour une fin de mandat. Pour certains

analystes, le mouvement est délibéré. Si l'administration Trump inscrit dans le marbre des positions très dures contre les entreprises chinoises, c'est pour que Joe Biden ait beaucoup de mal à revenir en arrière, sous peine d'être perçu comme faible vis-à-vis de Pékin.

L'affrontement sino-américain – technologique et commercial – se traduit déjà par une réorganisation des chaînes de production. Dans le nouveau contexte international, la Chine ne pourra plus être l'usine du monde. C'est en tout cas l'avis du patron de Foxconn, le géant taïwanais de l'électronique qui fabrique une grosse partie des iPhone d'Apple dans ses gigantesques usines de Shenzhen. Le dirigeant l'a expliqué sans détour aux investisseurs à l'été 2020. Comme lui, tous les fabricants d'électronique qui produisent aujourd'hui massivement en Chine réfléchissent à bâtir des usines au Vietnam, au Mexique, en Inde ou en Europe de l'Est. Il y avait une rationalité économique à tout produire en Chine. Mais entre la pandémie – qui a montré le danger d'être trop dépendant d'une seule zone de production – et les tensions géopolitiques, le risque est devenu trop grand. Apple aurait notamment demandé pour la première fois à Foxconn de produire des iPad et MacBook au Vietnam. Un « grand découplage » est à l'œuvre, au terme duquel il pourrait y avoir *a minima* deux chaînes d'approvisionnement technologiques complètement distinctes. La question de savoir qui en sortirait perdant reste ouverte.

Nombreux sont les critiques de la brutalité de Washington. Comme pour Huawei, ils craignent que dans son empressement à brider tout le secteur technologique chinois, Washington ne provoque l'effet inverse de celui escompté, c'est-à-dire un redoublement des efforts de Pékin pour ne plus dépendre en rien des technologies américaines. « Le seul effet de la politique de Trump à l'égard de la Chine, c'est d'avoir rendu la Chine plus autarcique, regrette par exemple Pascal Lamy, l'ex-directeur de l'Organisation mondiale du

commerce (OMC). Je considère, comme beaucoup, que la Chine, à certains égards, est une menace. Et je pense qu'une Chine autarcique est plus dangereuse qu'une Chine intégrée dans la mondialisation[10]. » L'honnêteté oblige à dire que l'ambition d'autonomie de Pékin préexistait à la crise actuelle. Dès 2015, le plan « Made in China 2025 » prévoyait de dépenser des milliards de dollars pour développer les compétences autochtones dans dix domaines clés (informatique, robotique, aviation, ferroviaire…). Les attaques américaines auront tout de même accéléré et légitimé le processus.

Back in the USSR

L'opposition frontale entre deux grandes puissances, idéologiquement incompatibles, et cherchant à se trouver des alliés dans le reste du monde, ne peut que rappeler la guerre froide. Dans un rapport publié en novembre 2020 et intitulé « Éléments du défi chinois[11] », le Département d'État l'écrit noir sur blanc : « Sur un aspect crucial, le défi chinois ressemble à celui présenté par l'Union soviétique au monde libre. » Pour les diplomates américains, le parallèle est essentiellement lié à la volonté de ces deux adversaires systémiques de construire un ordre mondial socialiste, dont ils seraient le centre. Avec cette différence fondamentale que l'URSS cherchait à imposer son modèle par la force militaire quand la Chine s'appuie surtout sur sa puissance économique. Cela rend le problème chinois plus délicat que le problème soviétique en un sens pour les États-Unis. Il leur est impossible de couper les ponts avec un maillon aussi central du commerce mondial.

Le rapport de 74 pages fait référence à deux reprises au « Long Telegram », un texte de février 1946 publié par George Kennan et qui

a jeté les bases de la politique américaine d'endiguement de l'Union soviétique. Pour certains commentateurs, les « Éléments du défi chinois » en sont un équivalent au XXIe siècle. Le rapport appelle de la même façon les États-Unis à prendre conscience de l'enjeu et à agir en conséquence. La liste des mesures préconisées va du maintien de la puissance militaire américaine au renforcement des alliances internationales, en passant par l'éducation des citoyens américains à l'ampleur du défi chinois ou la formation de fonctionnaires maîtrisant la langue et la culture chinoises. Le texte n'exclut pas, en dernier ressort, le recours à la force militaire. Dès sa sortie, un porte-parole du ministère chinois des Affaires étrangères a dénoncé un ramassis de mensonges antichinois rassemblés par des « fossiles vivants de la guerre froide », et voué à finir dans « la poubelle de l'Histoire »[12]. Mais cette critique est aussi une reconnaissance que les modes de pensée de la guerre froide sont bien de retour.

Pour les Américains, cet *aggiornamento* est d'abord un aveu d'échec. « Tout ce temps, nous avons pensé que le capitalisme amènerait la démocratie. Dans le cas de la Chine, nous avions tort », reconnaît Keith Krach, le nouveau débineur en chef de Huawei, qui reprend l'expression de son patron, Mike Pompeo : « Il est temps d'enlever nos lunettes roses et de traiter la Chine, non pas comme nous aimerions qu'elle soit, mais comme elle est réellement[13]. » Vingt ans plus tôt, lorsque le pays faisait son entrée à l'OMC, la conviction des Occidentaux était que l'ouverture économique se traduirait tôt ou tard par une ouverture politique. Le mur était tombé dix ans plus tôt. La « fin de l'histoire » avait été proclamée. Mais la prédiction était mauvaise. Alors que d'autres régimes durs d'Asie, comme la Corée du Sud ou Taïwan, se sont démocratisés, la Chine n'a pas fléchi. Au contraire, la certitude de la supériorité de son modèle s'est même renforcée. D'abord avec la crise financière de 2008. Le choc a montré

la fragilité du système capitaliste, qui n'a dû sa survie qu'à l'injection massive de capitaux par la Chine. À l'époque, Pékin a investi 600 milliards de dollars dans la construction d'infrastructures, baissé les impôts sur les entreprises, diminué son taux directeur d'un point – la plus forte baisse depuis la crise financière asiatique dix ans plus tôt… Au prix d'une bulle immobilière exceptionnelle, Pékin a alors sans doute sauvé l'économie mondiale. Dans le premier tome de ses mémoires, Barack Obama reconnaît lui-même qu'il avait alors trop besoin du soutien de la Chine pour l'affronter. De quoi raffermir d'éventuelles convictions communistes vacillantes à Pékin. L'arrivée au pouvoir en 2013 de Xi Jinping renforce encore cette détermination des autorités à éviter toute libéralisation. Le nouveau maître de Pékin est plus autoritaire que ses prédécesseurs – au point de faire voter en 2018 l'abolition de la limite des deux mandats de cinq ans que tous avaient respectée depuis Mao. Enfin, sans doute les troubles politiques de l'Occident des dernières années, du Brexit à l'élection de Donald Trump, ont-ils fini d'ancrer cette conviction. La Chine ne changera pas politiquement.

Économiquement, elle n'a par ailleurs jamais eu à regretter son choix. Son intégration au commerce mondial depuis trente ans s'est traduite par une trajectoire de croissance sans équivalent qui en a fait la deuxième économie et le premier centre manufacturier du monde. La projection de cette puissance à l'extérieur s'illustre dans le projet des « Nouvelles routes de la soie ». Lancé en 2013, ce plan titanesque dispose d'un budget avoisinant les 1 000 milliards de dollars pour investir dans les infrastructures d'une soixantaine de pays entre l'Asie, l'Europe et l'Afrique. C'est l'occasion pour les grands groupes chinois de muscler leurs exportations, et pour la Chine de promouvoir son modèle d'État fort et centralisé. Elle a de quoi plastronner. Cela fait belle lurette que la Chine n'est plus réduite au statut de fabricant bon

marché. Outre ses réussites dans les télécoms ou l'IA, le pays est également en pointe sur la fintech – autrement dit, les nouvelles méthodes de paiement dématérialisé. Tencent et Alibaba ont développé des plateformes financières ultra-performantes et fonctionnant à une échelle sans équivalent sur la planète. Elles s'exportent, notamment en Afrique, et offrent à la Chine une possibilité de remettre progressivement en cause l'hégémonie américaine sur les mouvements financiers mondiaux.

Ces performances inouïes signifient-elles que la Chine peut remporter son bras de fer avec les États-Unis ? « En Occident, nous avons tendance à surestimer les pouvoirs totalitaires. Ils nous impressionnent beaucoup. Et nous tendons aussi à exagérer nos propres fragilités[14] », nuance l'historien écossais Niall Ferguson, interrogé fin 2020 par le professeur de Berkeley Scott Galloway dans *The Prof G Show*. Selon lui, le pouvoir d'attraction des États-Unis et de l'Europe sur les individus ambitieux reste un atout déterminant, tandis que dans « un système non libre, où l'État de droit n'existe pas, où le parti est essentiellement au-dessus des lois, vous ne pouvez pas obtenir un résultat économique optimum ». L'universitaire en veut pour preuve l'annulation, à quarante-huit heures de l'échéance, de l'introduction en Bourse de Ant Financial, la filiale de paiements du groupe Alibaba. Prévue pour être la plus grosse opération de ce type jamais enregistrée, avec une levée de fonds de 34 milliards de dollars, elle a été décommandée dans la dernière ligne droite début novembre 2020 pour des motifs obscurs. Beaucoup y ont vu la volonté de Pékin de recadrer le groupe tech et son patron Jack Ma, en réaffirmant la primauté du politique sur les géants du numérique. La manœuvre interroge sur les capacités futures de ces groupes à innover et à accéder aux capitaux librement. Mais même sans rentrer dans ces considérations, la Chine a son lot de faiblesses : la croissance

économique ralentit, la population vieillit, l'endettement est énorme, le taux de pollution ravageur, et les problèmes de corruption et de répression des minorités sont autant de ferments de troubles sociaux… Enfin, puisque la nouvelle guerre froide se cristallise sur les technologies, le pays a un problème majeur, que les États-Unis ont cruellement mis en évidence avec Huawei : la Chine ne sait pas produire de puces électroniques haut de gamme – et ne sera probablement pas en mesure de le faire avant des années. Or ces minuscules composants sous-tendent toutes les technologies numériques. Même si la Chine est déterminée à tout faire pour combler son retard en la matière, ce pourrait bien être son talon d'Achille. Ou sa raison de rechercher un *modus vivendi* acceptable avec Washington.

Conclusion

Le 23 novembre 2020, le ministre chinois des Affaires étrangères Wang Yi appelle son homologue de l'Union européenne, Josep Borrell. Selon le compte-rendu officiel[1], il est question du Covid, du réchauffement climatique, mais aussi de la « nouvelle "guerre froide" », à laquelle Wang Yi exhorte Bruxelles de s'opposer, tout comme au « découplage », pour poursuivre l'« autonomie stratégique » de l'Europe. Le timing n'est pas innocent. Quelques heures plus tôt, les deux plus hauts représentants du bloc, la présidente de la Commission Ursula Von der Leyen et le président du Conseil Charles Michels, se sont entretenus avec Joe Biden, le président élu américain, pour l'inviter à « rebâtir une alliance forte entre les États-Unis et l'Europe[2] ». Après avoir été battue froid par Donald Trump pendant quatre ans, l'Europe mise sur un renouveau. La Chine, elle, espère bien que cela ne se fera pas à ses dépens. Le lendemain de ces coups de téléphone croisés à Bruxelles, c'est au tour d'Angela Merkel d'être appelée par Xi Jinping pour parler investissements et ouverture économique – une douce musique aux oreilles de la chancelière. Comme soixante ans plus tôt, l'Europe se retrouve au cœur d'un nouvel affrontement stratégique entre deux blocs. Jusqu'à présent, les pays du continent ont ménagé la chèvre et le chou. Dans le dossier de la 5G, ils ont répondu à l'appel de

Washington, en évitant au maximum de froisser Pékin. Alors que la fracture s'approfondit, sera-t-il possible de continuer à faire le grand écart ? Ou faudra-t-il choisir un camp ?

Pour certains, la position d'interface européenne est une opportunité à saisir. Xavier Niel, par exemple, assure voir une chance dans ce monde qui se coupe en deux. À l'automne 2020, le fondateur de Free s'en explique : « L'Europe est un territoire où ces deux blocs vont s'affronter. Quand TikTok vient bousculer Instagram, je trouve cela assez sain. Nous aurons le meilleur des deux mondes[3]. » En jouant habilement sur les deux tableaux, l'Europe pourrait-elle faire avancer ses propres intérêts ? Elle ne manque pas de sujets sur lesquels faire bouger les deux géants qui la courtisent. Sur le front commercial, elle partage les frustrations de l'Amérique concernant le protectionnisme déguisé et le dumping de la Chine, mais elle peste aussi contre les droits de douane imposés par les États-Unis sur ses produits. Elle a également des dossiers politiques à défendre, parmi lesquels l'Accord de Paris sur le climat ou celui sur le nucléaire iranien – dont l'ex-locataire de la Maison-Blanche s'est désengagé. Et sur le plan technologique, elle a de nombreux griefs à l'encontre de Washington. L'optimisation fiscale agressive des Gafa par exemple exaspère Bruxelles, tout comme le manque de considération des États-Unis pour les données personnelles des Européens. À deux reprises, la plus haute juridiction de l'Union a fait tomber les accords encadrant les transferts de données transatlantiques, jugeant que les lois américaines sur le renseignement permettent aux services secrets de faire main basse sur les données européennes sans contrôle… Le reproche est piquant. C'est peu ou prou ce que les États-Unis reprochent à la Chine avec sa propre loi sur le renseignement. Sur tous ces fronts, si les États-Unis veulent pouvoir compter sur le soutien de l'Europe dans son affrontement idéologique avec la Chine,

ils devront faire des concessions à l'Europe. Charge à celle-ci de jouer au mieux son avantage, en évitant une escalade délétère.

L'hypothèse d'un conflit violent ne peut être écartée. Le seul affrontement direct entre les armées américaines et chinoises remonte certes à la guerre de Corée (1950-1953), lorsque l'Armée populaire de libération était venue à la rescousse de la Corée du Nord, faisant des centaines de milliers de morts dans les rangs chinois, dont le propre fils de Mao. La mémoire de l'événement est restée vive en Chine, où l'anniversaire des soixante-dix ans du conflit, à l'automne 2020, a été marqué par de grandes célébrations. Xi Jinping en a profité pour livrer un discours violemment nationaliste, avertissant les États-Unis – sans les nommer – que son pays riposterait militairement à toute agression. Le dirigeant visait en particulier le soutien de Washington à Taïwan, un territoire dont Pékin refuse de reconnaître l'indépendance et que Xi Jinping a plusieurs fois menacé de reprendre par la force. Depuis l'élection à la présidence taïwanaise en 2016 de la candidate pro-indépendance Tsai Ing-wen, les tensions ont redoublé. Le soutien marqué de l'administration Trump n'a pas aidé : ventes d'armes à Taïwan, mais aussi visite à Taipei en août 2020 du secrétaire américain à la Santé – le plus haut responsable à se rendre sur l'île depuis quarante ans. Dans la mer de Chine du Sud, où l'US Navy patrouille pour assurer la « liberté de navigation », les bruits de bottes se font de plus en plus insistants. Pékin revendique la quasi-intégralité de la zone, au grand dam de ses voisins – Taïwan, la Malaisie, les Philippines, Brunei et le Vietnam. Dans cette poudrière, la fin de l'été 2020 a été marquée par des survols d'avions espions américains, des tirs de missiles balistiques chinois… et l'ajout à la « liste noire » du Département du commerce américain de 24 entreprises chinoises impliquées dans la construction d'îlots artificiels et d'installations militaires en pleine

mer depuis 2014. Hasard ou non, c'est en ce même été 2020 que l'Amérique a fini par priver *de facto* le champion technologique chinois Huawei de tout approvisionnement en puces haut de gamme. Le sujet n'a en théorie rien à voir. Sauf que Taïwan héberge les usines de TSMC – le seul industriel au monde à maîtriser la fabrication des composants électroniques les plus avancés. Cette malheureuse superposition des tensions – technologiques et géopolitiques – au-dessus de la petite île asiatique peut-elle suffire à déclencher les hostilités ?

Heureusement, toutes les parties y sont réticentes. La mer de Chine du Sud voit transiter un tiers du commerce maritime de la planète, et une proportion équivalente des cargaisons de pétrole brut, dont la Chine est le premier importateur mondial. Les risques économiques d'un conflit à cet endroit précis sont tellement énormes qu'une forme d'équilibre de la terreur pourrait s'établir. Sans compter que, selon certains experts, l'armée chinoise n'est pas encore en mesure d'affronter celle des États-Unis – même si ce n'est qu'une question de temps.

Cela permettra-t-il d'éviter le pire ? Pas nécessairement, explique l'universitaire américain Graham Allison dans *Vers la guerre*[4], un ouvrage très commenté aux États-Unis dès sa publication, au printemps 2017. Sa thèse est résumée sous une formule choc : le « piège de Thucydide », en référence à l'historien grec de l'Antiquité. Au Ve siècle avant notre ère, celui-ci analyse, dans *La Guerre du Péloponnèse*, les racines du conflit majeur entre Athènes et Sparte. Selon lui, c'est la peur provoquée chez la seconde – une puissance établie désirant le maintien du *statu quo* – par le rapide essor de la première – une puissance émergente percluse d'ambitions – qui les conduit inéluctablement à la guerre. Le « piège de Thucydide » va-t-il se refermer sur les deux grands rivaux du XXIe siècle ?

Une différence majeure avec l'Antiquité, mais aussi avec la première guerre froide, est l'existence de cordes de rappel, notamment économiques, pour éviter que l'opposition sino-américaine ne dégénère. Cela fait dire à l'ex-Premier ministre australien Kevin Rudd que, plutôt qu'une « guerre froide 2.0 », le conflit actuel est pour l'instant une « guerre froide 1.5[5] ». Pour l'ancien dirigeant, le pire peut être évité, à condition de trouver les mécanismes de régulation adéquats pour continuer à échanger, en cantonnant l'antagonisme au périmètre le plus restreint possible. Les bonnes volontés en ce sens ne manquent pas. « Nous devons tout faire pour éviter une nouvelle guerre froide », déclarait par exemple António Guterres fin septembre 2020, en ouverture de l'Assemblée générale des Nations unies[6]. La Chine ne cesse de déclarer publiquement qu'elle ne cherche pas l'affrontement. Et même aux États-Unis, des voix apaisantes se font entendre. Mi-novembre 2020, un rapport publié sous le titre « Meeting the China Challenge: A New Strategy for Technology Competition[7] », par 28 experts des plus grandes universités américaines (Yale, Berkeley, Stanford, Georgetown…), suggérait ainsi à la nouvelle administration Biden d'abandonner la politique d'exclusion totale prônée par Donald Trump au profit d'une stratégie plus nuancée, comportant trois volets : doper les capacités d'innovation des États-Unis, préserver l'ouverture des technologies à l'échelle mondiale et prendre des mesures très ciblées, y compris concernant Huawei, lorsque des risques de sécurité existent. Circonscrire le conflit aurait l'avantage de permettre aux deux antagonistes de collaborer sur des sujets essentiels comme la prolifération nucléaire, la santé publique mondiale, le réchauffement climatique… Vivre avec deux réseaux 5G, voire deux Internet distincts, ne sera pas commode. Mais sûrement

moins dangereux que des pandémies incontrôlables ou une planète en surchauffe.

Notes

Notes de l'avant-propos

1. « Video Released of Huawei Executive Meng Wanzhou Being Detained in Vancouver », YouTube, CBC News: The National, 20 août 2019.

2. Ferry Grijpink, Eric Kutcher, Alexandre Ménard, Sree Ramaswamy, Davide Schiavotto, James Manyika, Michael Chui, Rob Hamill et Emir Okan, « Connected World: An Evolution in Connectivity Beyond the 5G Revolution », Discussion paper, McKinsey Global Institute, février 2020.

Notes du chapitre premier

1. Ma Si, « First Remote Operation Carried out Using New Network », *China Daily*, 25 janvier 2019.

2. « First Remote Surgery in China Conducted Using 5G Technology », *Global Times*, 17 mars 2019.

3. Sébastien Dumoulin, « Le monde fabuleux de la 5G », *Les Échos week-end*, 5 mars 2019.

4. *Ibid.*

5. « Huawei and the 5G Ecosystem », Sinica Podcast, 16 juillet 2020.

6. « The Mobile Economy China 2020 », GSMA, 2020.

7. Fabienne Schmitt, Florian Dèbes, « Les conflits de demain vont être numériques, tous les grands États s'y préparent », *Les Échos*, 21 janvier 2020.

8. « Seven Iranians Working for Islamic Revolutionary Guard Corps-Affiliated Entities Charged for Conducting Coordinated Campaign of Cyber Attacks Against US Financial Sector », US Department of Justice, 24 mars 2016.

9. Ian Levy, « Security, Complexity and Huawei: Protecting the UK's Telecoms Networks », National Cyber Security Centre Blog, 22 février 2019.

10. *Ibid.*

Notes du chapitre II

1. John Pomfret, « Listening in on China's Telco Giant », *The Sydney Morning Herald*, 11 octobre 2010.

2. Yang Shaolong, *Huawei, une success-story à la chinoise*, Paris, Nuvis, 2016.

3. Hu Xiu, Table ronde II avec les médias chinois, 21 mai 2019.

4. Alexandra Harney, « Huawei: The Challenger from China », *Financial Times*, 10 janvier 2005.

5. China Business News, Table ronde I avec les médias chinois, 17 janvier 2019.

6. Evan S. Medeiros, Roger Cliff, Keith Crane, James C. Mulvenon, « A New Direction for China's Defense Industry », Rand Project Air Force, 2005.

7. Arjun Kharpal, interview par CNBC, 13 avril 2019.

8. « The Long March of the Invisible Mr Ren », *The Economist*, 2 juin 2011.

9. Karishma Vaswani, interview par BBC, 28 février 2019.

10. Sébastien Dumoulin, « Smartphones : Huawei veut se hisser sur les premières marches du podium », *Les Échos*, 16 octobre 2017.

11. *China Business Journal*, Table ronde II avec les médias chinois, 21 mai 2019.

12. Tammy Tam, « Ren Zhengfei's Interview with South China Morning Post », *Voices of Huawei*, 24 mars 2020.

13. Craig Matsumoto, « Cisco Says "No Way" to Nokia Rumor », *Light Reading*, 10 août 2005.

Notes du chapitre III

1. Sébastien Dumoulin, « Avec les techniciens télécoms, "héros des réseaux" », *Les Échos*, 2 avril 2020.

2. Eamon Barrett, *Fortune*, Table ronde avec les médias de différents pays, 15 janvier 2019.

3. Tom Mackenzie, Ren Zhengfei's interview with Bloomberg TV, 24 mai 2019.

4. Sébastien Dumoulin, « Linda Han, le nouveau visage de Huawei France », *Les Échos*, 9 septembre 2019.

5. Yang Shaolong, *Huawei, une success-story à la chinoise*, *op. cit.*

6. Tammy Tam, « Ren Zhengfei's Interview with South China Morning Post », art. cit.

7. Arjun Kharpal, interview cit.

8. Celia Chen, Li Tao, « Huawei Founder Ren Zhengfei Responds to HR Issues after Worker Complaints Go Viral Online », *South China Morning Post*, 6 novembre 2019.

9. Qianer Liu, Ryan McMorrow, « China's Huawei Faces Domestic Backlash over Detained Ex-Employee », *Financial Times*, 5 décembre 2019.

10. Raymond Zhong, « Jailed Huawei Workers Raised a Forbidden Subject: Iran », *The New York Times*, 25 avril 2020.

11. Yuan Yang, *Financial Times*, Table ronde avec les médias de différents pays, 15 janvier 2019.

12. *China Business Journal*, Table ronde II avec les médias chinois, cit.

13. Yuan Yang, *Financial Times*, Table ronde avec les médias de différents pays, cit.

14. Bianna Golodryga, Interview par CBS, 19 février 2019.

15. Justine Touraille, « Bal des debs : une fille du ciel dans la Ville lumière », *Paris Match*, 13 novembre 2018.

16. Tammy Tam, « Ren Zhengfei's Interview with South China Morning Post », art. cit.

17. « Huawei tira la casa por la venta para fichar a Messi », *Marketing Deportivo*, 14 mars 2016.

18. Classement Best Global Brands 2014, Interbrand.

19. Marie-Sophie Ramspacher, « François Quentin change de dimension avec Huawei », *Les Échos*, 26 novembre 2010.

20. Marc Cherki, « Huawei se défend face aux menaces de boycott en France », *Le Figaro*, 20 septembre 2012.

21. Harold Thibault, Solenn de Royer, « Dans les coulisses de la France China Foundation, pépinière à élites entre Paris et Pékin », *Le Monde*, 26 mai 2020.

22. Rapport d'activité 2018 du château de Versailles.

23. Frédéric Brun, « Le dîner de gala de la France China Foundation à Versailles », *Point de vue*, 28 juin 2018.

24. « Foreign Involvment in the Critical National Infrastructure: The Implications for National Security », Intelligence and Security Committee, juin 2013.

25. « Foreign Involvment in the Critical National Infrastructure: The Implications for National Security », Intelligence and Security Committee, juin 2013.

26. Ian Levy, « Security, Complexity and Huawei: Protecting the UK's Telecoms Networks », art. cit.

27. Fabienne Schmitt, Florian Dèbes, « Les conflits de demain vont être numériques, tous les grands États s'y préparent », art. cit.

28. « Huawei Cyber Security Transparency Centre Opens in Brussels », Huawei, 5 mars 2019.

29. Executive Research Associates (Pty) Ltd, « China in Africa: A Strategic Overview », Institute of Developing Economies, Japan External Trade Organization, octobre 2009.

30. Conférence « Mitigating Security Risks to Emerging 5G Networks », Center for Strategic & International Studies, 6 février 2019.

31. Fred P. Hochberg, « How the US Can Lead the World in Exports: Retooling Our Export Finance Strategy for the 21st Century », The Center for American Progress, 15 juin 2011.

32. Ken Hu, Deputy Chairman of Huawei Technologies, Chairman of Huawei USA, « Huawei Open Letter », *Wall Street Journal*, 5 février 2011 (https://online.wsj.com/public/resources/documents/Huawei20110205.pdf).

33. Chuin-Wei Yap, « State Support Helped Fuel Huawei's Global Rise », *The Wall Street Journal*, 25 décembre 2019.

34. Philippe Adnot, Jean-François Rapin, rapport général numéro 147 fait au nom de la commission des finances du Sénat, 22 novembre 2018.

35. Daisuke Wakabayashi, Brian X. Chen, « Apple, Capitalizing on New Tax Law, Plans to Bring Billions in Cash Back to US », *The New York Times*, 17 janvier 2018.

36. Rencontre avec la presse, ambassade des États-Unis à Paris, 22 janvier 2020.

37. Catherine Bertho-Lavenir (dir.), *L'État et les télécommunications en France et à l'étranger (1837-1987)*, Actes du colloque organisé à Paris les 3 et 4 novembre 1987 par l'École pratique des hautes études, IVe section et l'université Paris-Descartes-Paris V, Paris, Droz, 1991.

Notes du chapitre IV

1. James Bamford, « A Death in Athens », *The Intercept*, 29 septembre 2015.

2. Vassilis Prevelakis, Diomidis Spinellis, « The Athens Affair », *IEEE Spectrum*, 9 mars 2005.

3. Raymond Bonner, Christine Spolar, « Death in Singapore », *Financial Times*, 15 février 2013.

4. Jeremy Grant, « Todd Had Met Huawei Officials, Inquest Hears », *Financial Times*, 20 mai 2013.

5. Jeremy Grant, « Singapore Brushes off Concerns, Says Shane Todd Death Was Suicide », *Financial Times*, 8 juillet 2013.

6. T. Jasudasen, « Inquiry Was “Fair and Transparent” », Opinion, *Financial Times*, 17 juillet 2013.

7. Case of Tsalikidis and Others V. Greece, Requête 73974/14, arrêt de la Cour européenne des droits de l’homme, 16 novembre 2017.

8. Glenn Greenwald, « NSA Collecting Phone Records of Millions of Verizon Customers Daily », *The Guardian*, 6 juin 2013.

9. Glenn Greenwald, Ewen MacAskill, « NSA Prism Program Taps in to User Data of Apple, Google and Others », *The Guardian*, 7 juin 2013.

10. Laura Poitras, Marcel Rosenbach, Fidelius Schmid, Holger Stark, Jonathan Stock, « How the NSA Targets Germany and Europe », *Der Spiegel*, 1er juillet 2013.

11. Jacob Appelbaum, Laura Poitras, Marcel Rosenbach, Christian Stöcker, Jörg Schindler, Holger Stark, « Documents Reveal Top NSA Hacking Unit », *Der Spiegel*, 29 décembre 2013.

12. Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, New York, Metropolitan Books, 2014.

13. Sean Gallagher, « Photos of an NSA “Upgrade” Factory Show Cisco Router Getting Implant », Ars Technica, 14 mai 2014.

14. Daniel Thomas, Richard Waters, « Cisco Boss Calls on Obama to Rein in Surveillance », *Financial Times*, 18 mai 2014.

15. Don Clark, « Cisco CEO: Never Seen Such a Falloff in Orders », *Wall Street Journal*, 14 novembre 2013.

16. David E. Sanger, Nicole Perlroth, « NSA Breached Chinese Servers Seen as Security Threat », *The New York Times*, 22 mars 2014 ; « NSA Spied on Chinese Government and Networking Firm », *Der Spiegel*, 22 mars 2014.

17. « Slides Describe Mission Involving Huawei », *The New York Times*, 22 mars 2014.

18. David E. Sanger, Nicole Perlroth, « NSA Breached Chinese Servers Seen as Security Threat », art. cit.

19. Catalin Cimpanu, « Cisco Removed its Seventh Backdoor Account this Year, and that’s a Good Thing », ZDNet, 7 novembre 2018.

20. « Tenable Research Discovers Remote Code Execution Vulnerabilities in GPON Routers », Tenable Research, 27 février 2019.

21. Rapport annuel 2019 d’Ericsson.

22. « Advisory: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices », National Cyber Security Centre, 16 avril 2018.

23. « Huawei’s Chief Security Officer on 5G and Government Spying », Cyber podcast, 25 juin 2020.

24. David E. Sanger, Nicole Perlroth, « NSA Breached Chinese Servers Seen as Security Threat », art. cit.

25. « APT1: Exposing One of China's Cyber Espionage Units », Mandiant, février 2013.

26. « Five Chinese Military Hackers Charged: Indicted in Connection with Cyber Espionage Offenses against US », Federal Bureau of Investigation, 19 mai 2014.

27. « Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading US Aviation Companies », Department of Justice, 10 octobre 2018.

28. « Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018 », Department of Justice, 12 novembre 2020.

29. « Economic Espionage: FBI Launches Nationwide Awareness Campaign », Federal Bureau of Investigation, 23 juillet 2015.

30. « Remarks by the President to the Business Roundtable », The White House, 16 septembre 2015.

31. « Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information », Department of Justice, 20 décembre 2018.

32. Jack Stubbs, Joseph Menn, Christopher Bing, « Inside the West's Failed Fight against China's "Cloud Hopper" Hackers », Reuters, 26 juin 2019.

33. « Cybersecurity and American Power: Addressing New Threats to America's Economy and Military », American Enterprise Institute, 9 juillet 2012.

34. Christopher Wray, « The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States », Federal Bureau of Investigation, 7 juillet 2020.

35. Rencontre avec la presse, ambassade des États-Unis à Paris, 22 janvier 2020.

36. Joan Tilouine, Ghalia Kadiri, « À Addis-Abeba, le siège de l'Union africaine espionné par Pékin », *Le Monde Afrique*, 26 janvier 2018.

37. John Aglionby, Emily Feng, Yuan Yang, « African Union accuses China of Hacking Headquarters », *Financial Times*, 29 janvier 2018.

38. « Statement on Huawei's Work With the African Union », Huawei, 18 avril 2019.

39. Yuan Yang, *Financial Times*, Table ronde avec les médias de différents pays, cit.

40. Joe McDonald, Associated Press, Table ronde avec les médias de différents pays, 15 janvier 2019.

41. Joanna Plucinska, Koh Gui Qing, Alicja Ptak, Steve Stecklow, « Special Report: How Poland Became a Front in the Cold War between US and China », Reuters, 2 juillet 2019.

42. Weijing Wang, « Answers for Reuters Agency », Jankowski, Stroiński i Partnerzy, Reuters, 24 avril 2019 (www.reuters.com/investigates/special-report/assets/huawei-poland-spying/Wang_answers-for_special_report.pdf).

43. Stanisław Żaryn (@StZaryn), « Upon a decision of the court, the two suspects – Piotr D. and Weijing W. – have been arrested for the period of three months », Twitter, 11 janvier 2019.

44. Joanna Plucinska, Koh Gui Qing, Alicja Ptak, Steve Stecklow, « Special Report: How Poland Became a Front in the Cold War between US and China », art. cit.

Notes du chapitre v

1. « US and British Aircraft Attack Iraq », *The Guardian*, 16 février 2001.

2. « A Message from the Past for Baghdad », *The Economist*, 22 février 2001.

3. John Pomfret, Philip P. Pan, « Chinese Firm Is Focus of US Iraqi Suspicions », *The Washington Post*, 1er mars 2001.

4. Kelly Motz, Jordan Richie, « Sanctions Busting: Technology Two-Timing », *The Asian Wall Street Journal*, 19 mars 2001.

5. « Chinese firm denies report of helping Irak », AP, 2 mars 2001.

6. « Iraq Says Chinese Firm Pulls out of Phone Deal », Reuters, 9 septembre 2001.

7. « Pakistan Accepts US Battle Plan », Reuters, 15 septembre 2001.

8. François Hauter, « La Chine se range derrière les États-Unis », *Le Figaro*, 25 septembre 2001.

9. Y. P. Rajesh, « India Probes Unit of Chinese firm for Taliban Link », Reuters, 11 décembre 2001.

10. Elaine Kurtenbach, « Chinese Firm Denies Reports that Software Center in India helped Taliban », AP, 12 décembre 2001.

11. S. Srinivasan, « No Evidence of Taliban Links to Chinese Firm, Indian Authorities Say », AP, 15 décembre 2001.

12. Jeff Bounds, « China Firm Puts Main US Office in Plano », *Dallas Business Journal*, 30 juin 2002.

13. *Ibid.*

14. « Cisco's Motion for Preliminary Injunction », US District Court for the Eastern District of Texas, 5 février 2003.

15. Yang Shaolong, *Huawei, une success-story à la chinoise*, *op. cit.*

16. *Ibid.*

17. Rapport annuel 2005 de Cisco Systems.

18. Mark Chandler, « Cisco Suggests Huawei Release Court Report on Intellectual Property Misuse », Cisco Blogs, 1er octobre 2012.

19. Mark Chandler, « Huawei and Cisco's Source Code: Correcting the Record », Cisco Blogs, 11 octobre 2012.

20. Henny Sender, « How Huawei Tried to Sell itself to Motorola for $7.5bn », *Financial Times*, 27 février 2019.

21. Tom Mackenzie, interview cit.

22. Ren Zhengfei's Interview with Chinese Media, 21 mai 2019.

23. Tom Mackenzie, interview cit.

24. *Ibid.*

25. Phil Harvey, Peter Heywood, « Huawei Fires Supercomm Snooper », *Light Reading*, 17 août 2004 ; Superseding Indictment, United States v. Huawei Technologies Co., Ltd. et al, Cr. n° 18-457 (S-2) (AMD), 13 février 2020 ; Peter Burrows, avec Bruce Einhorn, « I Spy… A Spy From Huawei? », *Bloomberg*, 9 août 2004.

26. Christopher Rhoads, « Motorola Claims Huawei Plot », *The Wall Street Journal*, 22 juillet 2010.

27. Motorola, Inc. vs. Lemko Corp. *et al.*, Case Number 08 C 5427, United States District Court, Northern District of Illinois, 24 mai 2011.

28. Leena Rao, « Nokia Siemens Closes $975M Acquisition of Motorola Solutions' Wireless Network Assets », *Techcrunch*, 29 avril 2011.

29. « Chinese Telecommunications Device Manufacturer and its US Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice », Department of Justice, 28 janvier 2019.

30. Rachel Lerman, « Jury Awards T-Mobile $4.8M in Trade-Secrets Case against Huawei », *The Seattle Times*, 18 mai 2017.

31. Ashley Stewart, « Former Huawei Spokesman Recounts the AT&T Deal that Went Bust », *Puget Sound Business Journal*, 31 janvier 2019.

32. Conférence « Mitigating Security Risks to Emerging 5G Networks », cit.

33. Jeff Chase, Jon Zilber, *3Com: The Unsung Saga of the Silicon Valley Startup that Helped Give Birth to the Internet – and then Fumbled the Ball*, New York, BookBaby, 2019.

34. *Ibid.*

35. Richard Waters, James Politi, « Huawei-3Com deal finally collapses », *Financial Times*, 21 mars 2008.

36. Steven R. Weisman, « Sale of 3Com to Huawei Is Derailed by US Security Concerns », *The New York Times*, 21 février 2008.

37. Bill Hethcock, « Huawei Makes Plano Expansion Official », *Dallas Business Journal*, 11 novembre 2009.

38. John Pomfret, « Between US and China, a Trust Gap », *The Washington Post*, 8 octobre 2010.

39. *Ibid.*

40. « Ericsson, Alcatel Win 4G Telecoms Deal From AT&T », Reuters, 10 février 2010.

41. John Pomfret, « Between US and China, a Trust Gap », art. cit.

42. Spencer E. Ante, Shayndi Raice, « Dignitaries Come on Board to Ease Huawei Into US », *The Wall Street Journal*, 21 septembre 2010.

43. Joann S. Lublin, Shayndi Raice, « Security Fears Kill Chinese Bid in US », *The Wall Street Journal*, 5 novembre 2010.

44. Table ronde II avec les médias japonais, Shenzhen, 18 mai 2019.

45. Chris V. Nicholson, « The Big Chill: Huawei Imbroglio Puts Countries at Odds », *The New York Times*, 18 février 2011.

46. Ken Hu, « Huawei Open Letter », art. cit.

47. Mike Rogers, Dutch Ruppersberger, « Investigative Report on the US National Security: Issues Posed by Chinese Telecommunications Companies Huawei and ZTE », Permanent Select Committee on Intelligence, US House of Representatives, 8 octobre 2012.

48. Jim Wolf, « US Report Dashes China Telecoms' Expansion Hopes », Reuters, 8 octobre 2012.

49. John Suffolk, « Prism: Backtracking, Justifications, and the Shitty Shoe Shuffle, but how Will the World Respond? », johnsuffolk.typepad.com, 14 juin 2013.

Notes du chapitre VI

1. Ian Young, « Canadian Police Officer Says he Feared Huawei's Meng Wanzhou Would "Put up a Fight" During Arrest », *South China Morning Post*, 27 octobre 2020.

2. « Oral Reasons for Judgment », United States v. Meng, 2018 BCSC 2255, Supreme Court of British Columbia, 11 décembre 2018.

3. Denise Ryan, « Affidavit of Detained Huawei Official Details Life in Vancouver, Plans to Fight Extradition », *Vancouver Sun*, 11 décembre 2018.

4. Interview au *LA Times*, Shenzhen, 14 mars 2019.

5. « Sanctionned: The Arrest of a Telecom Giant », CBC podcast, 2019 ; « Five Things Disclosed in Latest Release of Documents in Meng Wanzhou's case », *The Canadian Press*, 24 septembre 2019 ; « Oral Reasons for Judgment », cit.

6. « Cathy Meng Spoke at Huawei ICT Finance Forum », Huawei, juin 2014.

7. « Oral Reasons for Judgment », cit.

8. *Ibid.*

9. « Sanctionned: The Arrest of a Telecom Giant », podcast cit.

10. « Oral Reasons for Judgment », cit.

11. « Sanctionned: The Arrest of a Telecom Giant », podcast cit.

12. « Oral Reasons for Judgment », cit.

13. Superseding Indictment, United States v. Huawei Technologies Co., Ltd., Huawei Device. Usa Inc., Skycom Tech Co. Ltd., Wanzhou Meng, Cr. n° 18-457 (S-2) (AMD), Eastern District of New York, 24 janvier 2019 ; Indictment, United States v. Huawei Technologies Co., Ltd., Huawei Device. Usa Inc., Cr. n° 19-010 (RSM), Western District of Washington At Seattle, 16 janvier 2019.

14. « Chinese Telecommunications Device Manufacturer and its US Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice », US Department of Justice, 28 janvier 2019.

15. Mike Rogers, Dutch Ruppersberger, « Investigative Report on the US National Security: Issues Posed by Chinese Telecommunications Companies Huawei and ZTE », art. cit.

16. Steve Stecklow, « Huawei Partner Offered Embargoed HP Gear to Iran », Reuters, 31 décembre 2012.

17. Steve Stecklow, « Huawei CFO Linked to Firm that Offered HP Gear to Iran », Reuters, 31 décembre 2013.

18. Jonathan Stempel, « HSBC wins OK of record $1.92 billion Money-Laundering Settlement », Reuters, 3 juillet 2013.

19. Karen Freifeld, Steve Stecklow, « HSBC Probe Helped Lead to US Charges against Huawei CFO », Reuters, 26 février 2019.

20. Superseding Indictment, United States v. Huawei Technologies Co., Ltd., Huawei Device. Usa Inc., Skycom Tech Co. Ltd., Wanzhou Meng, Cr. n° 18-457 (S-2) (AMD), Eastern District of New York, 24 janvier 2019.

21. Steve Stecklow, « Special Report: Chinese Firm Helps Iran Spy on Citizens », Reuters, 22 mars 2012.

22. « Secretary of Commerce Wilbur L. Ross, Jr. Announces $1.19 Billion Penalty for Chinese Company's Export Violations to Iran and North Korea », US Department of Commerce, 7 mars 2017.

23. *Ibid.*

24. « ZTE Corporation Document Submitted for Ratification (Review) Form », Bureau of Industry and Security, US Department of Commerce, 7 mars 2016.

25. « Order Activating Suspended Denial Order Relating to Zhongxing Telecommunications Equipment Corporation and Zte Kangxun Telecommunications Ltd. », Bureau of Industry and Security, US Department of Commerce, 15 avril 2018.

26. Elsa Conesa, « Trump confie la politique industrielle à Wilbur Ross, le "roi des faillites" », *Les Échos*, 30 novembre 2016.

27. Steve Stecklow, Karen Freifeld, Sijia Jiang, « US Ban on Sales to China's ZTE Opens Fresh Front as Tensions Escalate », Reuters, 16 avril 2018.

28. « Inside Information Announcement », ZTE Corporation, 9 mai 2018.

29. Yu Nakamura, « Choked by US Ban, ZTE Halts Smartphone Sales in China », *Nikkei Asia*, 9 mai 2018.

30. Donald J. Trump (@realDonaldTrump), « President Xi of China, and I, are working together to give massive Chinese phone company, ZTE, a way to get back into business, fast. Too many jobs in China lost. Commerce Department has been instructed to get it done! », Twitter, 13 mai 2018.

31. « Secretary Ross Announces $1.4 Billion ZTE Settlement; ZTE Board, Management Changes and Strictest BIS Compliance Requirements Ever », US Department of Commerce, 7 juin 2018.

32. Donald J. Trump (@realDonaldTrump), « ZTE, the large Chinese phone company, buys a big percentage of individual parts from US companies. This is also reflective of the larger trade deal we are negotiating with China and my personal relationship with President Xi », Twitter, 14 mai 2018.

33. Donald J. Trump (@realDonaldTrump), « Senator Schumer and Obama Administration let phone company ZTE flourish with no security checks. I closed it down then let it reopen with high level security guarantees, change of management and board, must purchase US parts and pay a $1.3 Billion fine. Dems do nothing… », Twitter, 26 mai 2018.

34. « Remarks by US Commerce Secretary Wilbur L. Ross at the Department of Justice Announcement on National Security Related Criminal Charges Against Chinese Telecommunications Conglomerate Huawei », US Department of Commerce, 28 janvier 2019.

35. Jeff Mason, Steve Holland, « Trump Says he Could Intervene in US Case against Huawei CFO », Reuters, 12 décembre 2018.

36. « Remarks of the Spokesperson of the Chinese Embassy in Canada on the Issue of a Chinese Citizen Arrested by the Canadian Side », Embassy of the People's Republic of China in Canada, 6 décembre 2018

37. « Sanctionned: The Arrest of a Telecom Giant », podcast cit.

38. Jason Proctor, « Premature Victory Lap? Meng Wanzhou Poses Ahead of Momentous Court Decision », CBC, 25 mai 2020.

39. Gao Yuan (@GaoYuan86), « On top of Ren's desk packed with company files, newspapers and business cards, there is a translated version of "Le Piège Americain," or "The American Trap". Written by former Alstom executive Frederic Pierucci about his 5-yr battle with the @TheJusticeDept », Twitter, 27 mai 2019.

40. Frédéric Pierucci, Mathieu Aron, *Le Piège américain*, Paris, Lattès, 2019.

41. Qingqing_Chen (@qingqingparis), « Yes, #RenZhengfei is now asking every #Huawei ers to read this book. In a cafeteria at Huawei's Songshanhu manufacturing base, there's a promoting banner for this book, calling it "Huawei-like incident in France" », Twitter, 28 mai 2019.

42. Hearing before the Select Committee on Intelligence of the US Senate, 13 février 2018.

43. Interview avec CTV, 13 mars 2019.

44. « Commerce Department Further Restricts Huawei Access to US Technology and Adds Another 38 Affiliates to the Entity List », US Department of Commerce, 17 août 2020.

45. Yuan Yang, « Huawei's Revenue Growth Slows as US Tightens Sanctions », *Financial Times*, 23 octobre 2020.

46. Tim Culpan, « Trump Just Took the Nuclear Option on Huawei », *Bloomberg Opinion*, 18 août 2020.

Notes du chapitre VII

1. Chris Uhlmann, Angus Grigg, « Secret Spy Dinner Seals Huawei Fate », *The Australian Financial Review*, 14 décembre 2018 ; Chris Uhlmann, Angus Grigg, « How the "Five Eyes" Cooked up the Campaign to Kill Huawei », *The Sydney Morning Herald*, 13 décembre 2018 ; Robert Fife, Steven Chase, « Five Eyes Spy Chiefs Warned Trudeau Twice about Huawei National-Security Risk », *The Globe and Mail*, 17 décembre 2018.

2. Mark Hosenball, « White House Campaigns to win Senate confirmation of CIA nominee », Reuters, 3 mai 2018 ; John Rizzo, « Company Man: Thirty Years of Controversy and Crisis in the CIA », Simon and Schuster, 2014 ; « Open Hearing: Nomination of Gina Haspel to Be the Director of the Central Intelligence Agency », Select Committee on Intelligence of the United States Senate, 9 mai 2018.

3. Huawei Australia (@HuaweiOZ), « We have been informed by the Govt that Huawei & ZTE have been banned from providing 5G technology to Australia. This is a extremely disappointing result for consumers. Huawei is a world leader in 5G. Has safely & securely delivered wireless technology in Aust for close to 15 yrs », Twitter, 23 août 2018.

4. « Huawei Marine Signs Submarine Cable Contract in Solomon Islands », Huawei, 7 juillet 2017.

5. Australian Signals Directorate (@ASDGovAu), « Hi Internet, ASD here. Long time listener, first time caller », Twitter, 29 octobre 2018.

6. « Then and Now: Coming out from the Shadows », Director-General ASD speech to Aspi National Security Dinner, Australian Strategic Policy Institute, 29 octobre 2018.

7. « GCSB Declines Spark's Proposal to Use Huawei 5G Equipment », Spark, 28 novembre 2018.

8. Alex Younger, discours, University of St Andrews, 3 décembre 2018.

9. Interview au magazine *Time*, Shenzhen, 12 avril 2019.

10. Mike Burgess (@MikePBurgess), « Thanks for sharing. In my business I've never seen anything "fully isolated…" », Twitter, 21 novembre 2018.

11. Robert Fife, Steven Chase, Colin Freeze, « CSIS Director Warns of State-Sponsored Espionage threat to 5G Networks », *The Globe and Mail*, 4 décembre 2018.

12. « Allocution de David Vigneault au Economic Club of Canada », Service canadien du renseignement de sécurité, 4 décembre 2018.

13. « Oral Evidence: UK Telecommunications Infrastructure and the UK's Domestic Capability, HC 450 », Science and Technology Committee, House of Commons, 28 octobre 2020.

14. Basile Dekonink, « Les télécoms, le grand pari du patron de Rakuten Hiroshi Mikitani », *Les Échos*, 6 janvier 2020.

15. « Understanding the Market for 4G RAN in Europe: Share of Chinese and Non-Chinese Vendors in 102 Mobile Networks », Strand Consult, 2020.

16. Paul Smith, « Huawei Reveals $100m Local Cost of "Cold War" », *Australian Financial Review*, 22 septembre 2020.

17. « Software i hardware společností Huawei a ZTE je bezpečnostní hrozbou », *Núkib*, 17 décembre 2018.

18. « Czech Cyber Chief Expects Huawei, ZTE to Be Excluded from More Tenders », Reuters, 5 février 2019.

19. « Czech President Welcomes Huawei's Participation in 5G Deployment », Huawei, 27 avril 2019.

20. Keegan Elmer, « Czech Cybersecurity Chief Fired Amid Dispute over Huawei Security Threat », *South China Morning Post*, 17 décembre 2019.

21. Bojan Pancevski, Sara Germano, « Drop Huawei or See Intelligence Sharing Pared Back, US Tells Germany », *The Wall Street Journal*, 11 mars 2019.

22. Présentation de Mike Pompeo sur le site web de l'ambassade des États-Unis en France.

23. Raphaël Balenieri, Sébastien Dumoulin, « La France temporise sur le dossier Huawei », *Les Échos*, 7 décembre 2018.

24. « Déclaration du porte-parole de l'ambassade de Chine en France sur la question de Huawei et de la 5G », ambassade de Chine en France, 9 février 2020.

25. Simon Kruse, Lene Winther, « Banned Recording Reveals China Ambassador Threatened Faroese Leader at Secret Meeting », Berlingske, 10 décembre 2019.

26. Tony Czuczka, Steven Arons, « China Threatens Retaliation Should Germany Ban Huawei 5G », Bloomberg, 15 décembre 2019.

27. Gino Chouinard, Georges Pothier, « Le bilan de fin d'année de Justin Trudeau », *Salut Bonjour*, TVA, 19 décembre 2019.

28. Fabienne Schmitt, « Orange, contre l'interdiction de Huawei en France », *Les Échos*, 23 janvier 2020.

29. Sébastien Dumoulin, « Huawei : le coût d'une exclusion des réseaux télécoms fait débat », *Les Échos*, 14 juillet 2020.

30. Conférence de presse en ligne avec le sous-secrétaire d'État Keith Krach, US Department of State, 30 septembre 2020.

31. Amy Kazmin, Stephanie Findlay, « India Moves to Cut Huawei Gear from Telecoms Network », *Financial Times*, 24 août 2020.

Notes du chapitre VIII

1. Robert Fife, Steven Chase, « Chrétien Proposes Cancelling Meng's Extradition Case to Unfreeze Relations with China », *The Globe and Mail*, 13 juin 2019.

2. « China Cables », Icij, 24 novembre 2019.

3. « Oral Evidence: UK Telecommunications Infrastructure, HC 2200 », Science and Technology Committee, House of Commons, 10 juin 2019.

4. Fergus Ryan, Danielle Cave, Vicky Xiuzhong Xu, « Mapping more of China's Technology Giants: AI and Surveillance », International Cyber Policy Centre, The Australian Strategic Policy Institute, novembre 2019.

5. Interview au *Globe and Mail*, 2 décembre 2019.

6. Olivier Tesquet, « Amesys : les tribulations égyptiennes d'un marchand d'armes numériques français », *Télérama*, 5 juillet 2017.

7. Interview au *LA Times*, art. cit.

8. *Ibid.*

9. Elsa Kania, « Much Ado about Huawei (part 2) », The Strategist, The Australian Strategic Policy Institute, 28 mars 2018 ; Jeffrey Enderson (Professor emeritus of international development, University of Bristol), « Who Really Pulls the Strings at Huawei? », *The Guardian*, 26 avril 2019.

10. Huawei, rapport annuel 2019.

11. Christopher Balding, Donald C. Clarke, « Who Owns Huawei? », *Social Science Research Network*, 17 avril 2019.

12. Raymond Zhong, « Who Owns Huawei? The Company Tried to Explain. It Got Complicated », *The New York Times*, 25 avril 2019 ; Yuan Yang, « Huawei Says Employees Control Company Through "Virtual Shares" », *Financial Times*, 25 avril 2019.

13. Peggy Sito, « By Letting Staff Share Huawei's Stock and Profit, Ren Zhengfei Instils Kinship and Unleashes Telecom Giant's "Wolf Culture" », *South China Morning Post*, 9 avril 2020.

14. Northern European Media Roundtable, 15 octobre 2019.

15. Solveig Godeluck, « François Quentin (Huawei) : "Nous croyons beaucoup à l'Europe" », *Les Échos*, 11 février 2013.

16. Interview avec CBS, 19 février 2019.

17. Interview au Handelsblatt, 11 avril 2019.

18. Interview à Bloomberg TV, 24 mai 2019.

19. Table ronde avec les médias de différents pays, Shenzhen, 15 janvier 2019.

20. Interview au *LA Times*, art. cit.

21. Conférence de presse de Robert Strayer (Département d'État) et Adam Hickey (Département de la justice), ambassade de France à Paris, 22 janvier 2020.

22. Interview par CNN, Shenzhen, 13 mars 2019.

23. « The Chinese Communist Party's Ideology and Global Ambitions », Remarks delivered by National Security Advisor Robert C. O'Brien, The White House, 26 juin 2020.

24. Rencontre avec la presse à l'ambassade américaine à Paris, 2 décembre 2019.

25. Lucie Robequain, « Terrorisme : Apple refuse de collaborer avec le FBI », *Les Échos*, 18 février 2016.

26. Rencontre avec la presse à l'ambassade américaine à Paris, 2 décembre 2019.

27. *China Business Journal*, Table ronde II avec les médias chinois, cit.

28. « Forging Ahead to Survive and Thrive: A New Year's Message for 2020, Eric Xu, Rotating Chairman », Huawei, 31 décembre 2019.

29. Sébastien Dumoulin, « Huawei lance en France sa première usine hors de Chine », *Les Échos*, 27 février 2020.

30. « Huawei Asks Court to Overturn FCC Order on Government Subsidy Program », Huawei, 5 décembre 2019.

31. Boris Jancic, « Huawei Tries Rugby Charm in NZ After Ban », AAP, 13 février 2019.

32. « Welcome Address by Abraham Liu, Chief Representative of Huawei to the EU Institutions, at the Digitall 2019 Chinese New Year Celebration », Huawei, 7 février 2019.

33. Gareth Corfield, « We're Great, Boasts Huawei in Founder's Little Red Book – But Isn't that a Video Game Screenshot? », *The Register*, 30 août 2019.

34. Table Ronde II avec les médias chinois, Shenzhen, 21 mai 2019.

35. Zhang Zhihao, « Huawei's Workers Tell their Stories of Resilience, Solidarity », *China Daily*, 25 mai 2019.

36. Global Times (@globaltimesnews), « How Chinese residents show their support to #Huawei? Singing! A video "Huawei Beauty" which features children singing lyrics supporting Huawei went viral. Lyrics include "we love our country, we love homegrown brand Huawei" and "China's homegrown chips are the most valuable one" », Twitter, 27 février 2019.

37. *China Business Journal*, Table ronde II avec les médias chinois, cit.

38. Sijia Jiang, « Huawei Challenges US Defense Bill as Sanctions Fight Ramps up », Reuters, 29 mai 2019.

Notes du chapitre IX

1. Interview au magazine *Time*, Shenzhen, 12 avril 2019.

2. « Fact Finding Study on Patents Declared to the 5G Standard », IPlytics, janvier 2020.

3. Yifan Yu, « US to Allow Companies to Work with Huawei on 5G Standards », *Nikkei Asia*, 16 juin 2020.

4. Paul Mozur, Edmund Lee, « Huawei Is Said to Demand Patent Fees from Verizon », *The New York Times*, 12 juin 2019.

5. Steven Levy, « Huawei, 5G, and the Man Who Conquered Noise », *Wired*, 16 novembre 2020.

6. Dominique Lazanski, « China, Huawei and 5G Standards in the UK », *Forbes*, 27 avril 2019.

7. « Towards a New Internet for the Year 2030 and Beyond », présentation de Richard Li, Chief Scientist Future Networks Huawei USA, devant l'UIT, 18 juillet 2018.

8. Anna Gross, Madhumita Murgia, « China and Huawei Propose Reinvention of the Internet », *Financial Times*, 27 mars 2020.

9. Gordon Corera, « The New Tech Cold War », *Seriously*, BBC Radio 4, 19 juin 2020.

10. « On n'arrête pas l'éco », France Inter, 7 novembre 2020.

11. « The Elements of the China Challenge », The Policy Planning Staff, Office of the Secretary of State, novembre 2020.

12. « China slams US paper containing anti-China lies », Xinhua, 19 novembre 2020.

13. Conférence de presse en ligne avec le sous-secrétaire d'État Keith Krach, US Department of State, 30 septembre 2020.

14. Scott Galloway, « Cold War II: China Tech vs. US Tech », *The Prof G Show*, 5 novembre 2020.

Notes de la conclusion

1. « Wang Yi Speaks with High Representative of the EU for Foreign Affairs and Security Policy Josep Borrell on the Phone », Ministère des Affaires étrangères de la République populaire de Chine, 23 novembre 2020.

2. Charles Michel (@eucopresident), « Let's rebuild a strong #EU #USA alliance. I just spoke to President-elect @JoeBiden and invited him to a special meeting in Brussels next year with #EU27 Now is the time to join forces on #COVID19 #climate #security #multilateralism », Twitter, 23 novembre 2020.

3. Sébastien Dumoulin, David Barroux, Fabienne Schmitt, « Xavier Niel : “Ce qui pollue, ce n’est pas la 5G mais nos smartphones” », *Les Échos*, 16 octobre 2020.

4. Graham Allison, « Destined for War: Can America and China Escape Thucydides’s Trap? », *Mariner Books*, mai 2017.

5. « US v China: A New Cold War? », The Real Story, BBC World Service, 30 octobre 2020.

6. António Guterres, « Address to the Opening of the General Debate of the 75th Session of the General Assembly », United Nations Secretary-General, 22 septembre 2020.

7. « Meeting the China Challenge: A New American Strategy for Technology Competition », Working Group on Science and Technology in US-China Relations, 21st Century China Center, 16 novembre 2020.

Retrouvez tous nos ouvrages
sur www.tallandier.com